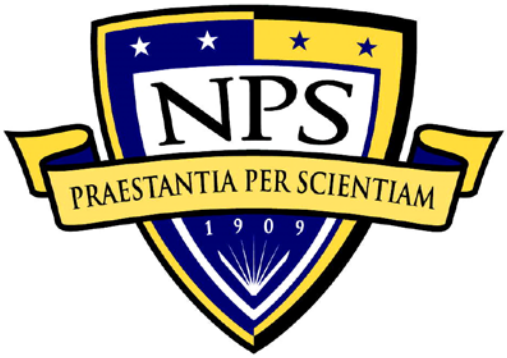

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPLEMENTING CYBER COERCION

by

Clinton M. Woods

March 2015

Thesis Advisor:	Neil C. Rowe
Second Reader:	Dorothy E. Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2015	Master's Thesis

4. TITLE AND SUBTITLE
IMPLEMENTING CYBER COERCION

5. FUNDING NUMBERS

6. AUTHOR(S) Woods, Clinton M.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Cyberspace has become an essential component of modern militaries. As this dependency grows, militaries who exploit this dependency may be able to hurt their adversaries within cyberspace to coerce them into a desirable action. This thesis will explore one particular use of cyber coercion, the use of cyber weapons to target supply chains, to study what methods may be best suited for cyber coercion.

This thesis first looks at the possibilities for cyber coercion and the various factors that are important for an attack method to successfully coerce an adversary, including reusability, reversibility, and legality. It then proposes various cyber attacks that could be used in cyber coercion and reviews factors important in cyber coercion. Next, it takes these proposed methods and walks through three scenarios against fictional nation-states to analyze how these methods might perform in a cyber-coercion operation. Included are possible effects if these same attacks were used against the United States. Findings are then presented based on the scenarios.

14. SUBJECT TERMS	15. NUMBER OF PAGES
cyber coercion, cyber warfare, cyber policy	97
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IMPLEMENTING CYBER COERCION

Clinton M. Woods
Lieutenant, United States Navy
B.S., Texas A&M University, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2015

Author: Clinton M. Woods

Approved by: Neil C. Rowe
Thesis Advisor

Dorothy E. Denning
Second Reader

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cyberspace has become an essential component of modern militaries. As this dependency grows, militaries who exploit this dependency may be able to hurt their adversaries within cyberspace to coerce them into a desirable action. This thesis will explore one particular use of cyber coercion, the use of cyber weapons to target supply chains, to study what methods may be best suited for cyber coercion.

This thesis first looks at the possibilities for cyber coercion and the various factors that are important for an attack method to successfully coerce an adversary, including reusability, reversibility, and legality. It then proposes various cyber attacks that could be used in cyber coercion and reviews factors important in cyber coercion. Next, it takes these proposed methods and walks through three scenarios against fictional nation-states to analyze how these methods might perform in a cyber-coercion operation. Included are possible effects if these same attacks were used against the United States. Findings are then presented based on the scenarios.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACK	acknowledgment
APT	advanced persistent threat
BBC	British Broadcasting Corporation
CDRUSCYBERCOM	Commander, United States Cyber Command
CERT	Computer Emergency Response Team
CPU	central processing unit
CSRF	cross-site request forgery
DDOS	distributed denial of service
DNS	domain name system
DOD	Department of Defense
DOJ	Department of Justice
DOS	denial of service
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
HP	Hewlett Packard
ICMP	Internet control message protocol
IETF	Internet Engineering Task Force
IP	Internet protocol
ISIL	Islamic State of Iraq and the Levant
ISP	Internet service provider
JP	Joint Publication
MTU	maximum transmission unit
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NMCI	Navy Marine Corps Intranet
NPS	Naval Postgraduate School
NSA	National Security Agency
OSD	Office of the Secretary of Defense
PCCW	Pacific Century CyberWorks
PLA	People’s Liberation Army

RFC	request for comment
RFID	radio frequency identification
RIPE NCC	Réseaux IP Européens Network Coordination Centre
SCADA	supervisory control and data acquisition
SYN	sequence
TCP	transmission control protocol
U.N.	United Nations
U.S.	United States
USCYBERCOM	United States Cyber Command

ACKNOWLEDGMENTS

01010100011011110010000001101101011110010010000001110111011
0100101100110011001010010110000100000010000110110000101110100011
0100001100101011100100110100101101110011001010010110000100000011
0011001101111011100100010000001101000011001010111001000100000011
0110001101111011101100110010100100000011000010110111001100100001
0000001110011011101010111000000111000000110111101110010011101000001
0000001110100011010000111001001101111011101010110011101101000011
0111101110101011101000010000001101101011110010010000001110100011
0100101101101011001010010000001100001011101000010000001001110010
1000001010011001011100010000001010100011011110010000001010000011
1001001101111011001100110010101110011011100110110111101110010001
0000001010010011011110111011101100101001000000110000101101110011
0010000100000010100000111001001101111011001100110010101110011011
1001101101111011100100010000001000100011001010110111001101110011
0100101101110011001110010110000100000011001100110111101110010001
0000001110000001110010011011110111011100110100101100100011010010110
0111001100111001000000111010001101000011001010110100101110010001
0000001110100011010010110110101100101001011000010000001110010011
0010101100011011011110110110101101101011001010110111001100100011
0000101110100011010010110111101101110011100110010110000100000011
0000101101110011001000010000001110000011001010111001001110011011
1000001100101011000110111010001101001011101100110010101110011001
0000001101001011011100010000001110000011100100110010101110000011
0000101110010011010010110111001100111001000000111010001101000011
0100101110011001000000111010001101000011001010111001101101001011
1001100101110

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The world remains a volatile place. Multiple countries are engaged in a long-standing territorial dispute in the South China Sea. Separatists have led uprisings in Crimea and other eastern Ukrainian regions. Populist uprisings continue throughout the Middle East since the commencement of the Arab Spring. The Islamic State of Iraq and the Levant (ISIL) has gained control of territory in both Iraq and Syria and has killed several Western and allied-country hostages. Recent attacks on Sony Pictures attributed to North Korea have reminded us that these threats are not isolated to the physical world. Highlighting the threats faced in cyberspace, the Department of Justice (DOJ) indicted five Chinese military hackers for their role in cyber operations against U.S. corporations. During his Senate confirmation hearing for Secretary of Defense, Leon Panetta warned, “the next Pearl Harbor that we confront could very well be a cyber attack” (Mulrine, 2011). The threat from cyber attacks continues to grow as dependency of the Internet has increased. Though Symantec (2014) reported that cyber attacks were down in 2013 compared to 2012, the focus and persistence of the attacks increased. The United States needs to be prepared for these attacks and to utilize cyber operations to its advantage.

B. GOAL AND PURPOSE

Coercion is using threats or force to persuade another to do something. This can be in the form of either deterrence, preventing another from taking an action, or compellence, encouraging another to revert from a position taken. Many argue that deterrence is not effective in cyberspace as nuclear weapons were during the Cold War. Deterrence in the Cold War era worked because both sides knew that an attack would be met with retaliation. Thus, both sides were deterred from taking actions which the other side was strongly against. Then Deputy Secretary of Defense William Lynn wrote while describing the United

States cyber strategy, “it must also recognize that traditional Cold War deterrence models of assured retaliation do not apply to cyberspace, where it is difficult and time consuming to identify an attack’s perpetrator. Whereas a missile comes with a return address, a computer virus generally does not” (Lynn, 2010, p. 99). Others have argued that deterrence is effective in cyberspace and the lack of large scale cyber attacks between nation-states is a testimony of that deterrence (Healey, 2014). That deterrence cannot be expected to prevent all cyber attacks, but instead creates a ceiling which nation-states keep their cyber attacks under. Given that attribution is not as obvious or easily determined as with a kinetic attack, cyber weapons are readily available and can be used by non-nation-state actors who are hard to retaliate against, and the difference between espionage and a cyber attack is not clear, this paper will view cyber coercion from the vantage point of the United States compelling an adversary, verses a deterrence model. By applying force, one applies a little pain to demonstrate resolve and ability to cause more pain, and hopefully force the adversary to take the desired action. However, knowing how and where to apply the force is important. This paper will review both what force should be used and where to apply it to achieve cyber coercion.

The supply chain of a military provides for all the needs of the military. Weapons, food, and material goods are all made, procured, and supplied using supply chains. Finding a weak point within supply chains can allow for the opportunity to cause the supply chains to break. Without supply chains, a military might not be able to continue to conduct operations. This makes it a good candidate for targeting in cyber coercion. However, supply chains may be flexible and resilient. Finding weak points that are essential is key to a successful attack. This paper will discuss and analyze potential targets within the supply chain.

Though the desired effect of coercion is for one’s adversary to completely give in to the demands, this is not always the outcome. That does not mean the coercion failed, though. If a cyber coercion attack brings an adversary to the bargaining table that would be a positive benefit. However, does the cyber

operation run the risk of escalating hostilities? Could it cause a cyber war to break out? Knowing what attack to use and where to apply it is important, but just as important is estimating the potential effect of the attack. This paper will review possible cyber tools to be used in a cyber coercion operation and discuss where those tools would best be applied within the context of targeting military supply chains. A heavy focus will be given to reversible tools, cyber weapons that when their use is terminated, can restore the status of the data or network to it same condition before the attack. This thesis will then apply three of these tools to various scenarios targeting different adversarial countries of different military and cyber capabilities. The potential response by the adversary will gauge the effectiveness of the attack with the adversary capitulating or being driving to the negotiating table to be considered positive results, and increased escalations to be considered negative results.

C. APPLICABILITY TO THE DEPARTMENT OF DEFENSE

After 14 years at war, the U.S. Department of Defense (DOD) needs to find methods that allow it to exert influence around the world while not overexerting the force. In his 2015 State of the Union address, U.S. President Barack Obama posed two questions as to the direction of the U.S. power in the future, “Will we approach the world fearful and reactive, dragged into costly conflicts that strain our military and set back our standing? Or will we lead wisely, using all elements of our power to defeat new threats and protect our planet?” The cyber methods analyzed in this thesis will allow the United States to defeat new threats without costly conflicts exerting their toll on budgets and military forces.

Addressing the students of the Naval Postgraduate School (NPS) in February 2015, Director of the National Security Agency (DIRNSA) and Commander, U.S. Cyber Command (CDRUSCYBERCOM), Admiral Michael Rogers, said that cyber needs to present a target package to combatant commanders illustrating the weapon, the target, the expected damage to the

target, and the expected collateral damage. This allows the combatant commanders and other decision makers to make the best possible decision of what course of action to take for the desired effect. This process takes time and effort and cannot be easily done on the fly. This thesis furthers this process for cyber, by describing weapons, presenting several potential targets, analyzing the damage expected by the weapons, discussing possible collateral damage, and reviewing possible and likely responsive courses of action by the adversary. Of especial consideration is the use of reversible weapons, which allow the military to conduct an attack and quickly, and then restore the target to its pre-attack condition. This is not something that can be achieved through kinetic force.

The use of reversible weapons holds great potential for the military. In the aftermath of recent conflicts, the United States has spent large amounts in rebuilding infrastructure destroyed in the conflict. For example, in Iraq, over $60 billion has been spent in rebuilding infrastructure (Mulrine, 2013). Not only is rebuilding costly, but a lengthy or problematic process can cost the hearts and minds of the civilians of the adversarial nation. If attacks which could be reversed were used, these costs would not only be reduced, since the infrastructure does not need to cost as much to rebuild, the ability of the United States to quickly restore services after the conflict could improve, and the standing of the United States with the citizens improved. Cyber weapons have the potential of being able to drive a desired effect, even preventing the use of infrastructure, without physically destroying the infrastructure. This is an effect that kinetic weapons do not have. Cyber attacks analyzed in this paper will be analyzed for their reversibility after the conflict is terminated.

These same tactics may be used against the United States. The DOD needs to understand the effects of such attacks to prepare for defending them. Each scenario reviewed will include an analysis of possible effects if such an attack were used against the United States.

Coercion is not a new tactic and is one the military is quite familiar with. War has been likened to “organized coercion” (Freedman, 1998). However,

coercive methods that can allow the United States to achieve superiority or deny adversarial activity in a domain or capacity to accomplish a political objective without having to resort to full-scale war are very important. This study will further the understanding of cyber coercion for the military by applying three cyber coercion operations in a scenario of military context. Given a continuing volatile world, cyber coercion allows the U.S. military to project power in ways other than kinetic force.

D. OUTLINE

The thesis is organized into five chapters. Chapter I introduces the study, provides the goals and purpose, and provides the relevance to the DOD. Chapter II defines cyber coercion and reviews the components of cyber coercion which help make it successful. Chapter III reviews various methods of cyber attacks which can target the supply chain. Chapter IV analyzes the use of three of the methods in three scenarios pitting the United States against an adversary of various capabilities. Chapter V concludes the paper, providing a summary of the findings and recommending future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DEFINING CYBER COERCION

A. DEFINING COERCION

On November 22, 2014, computers at Sony Pictures began displaying messages along with images of skulls threatening to release private information that had been gained by a hacking group (“The Interview,” 2014). This hacking group, called the Guardians of Peace, released compromised Sony Pictures emails, unreleased movies, and financial documents, causing embarrassment to Sony Pictures and many members of the film industry whose private emails and information were displayed publicly. The group then escalated their fight by announcing they would conduct terrorist attacks on any movie theater showing an upcoming movie, *The Interview*, a film mocking North Korean leader, Kim Jong-un. Citing the terror threats, Sony canceled the release of the movie, which President Barack Obama called “a mistake” (Bradner, 2014). Though Sony later reversed their position and released the movie in theaters and online, the effect of cyber coercion was demonstrated. The FBI attributed the attack back to North Korea. President Obama recognized this threat, saying, “if we set a precedent in which a dictator in another country can disrupt through cyber, a company’s distribution chain or its products, and as a consequence we start censoring ourselves, that’s a problem” (Bradner, 2014).

Coercion is legally defined as “any form of compulsion or constraint which compels or induces a person to act otherwise than freely” (Gifis, 1991, p. 78). Cyber coercion is the application of coercion to cyberspace. By using cyber weapons, one can use, or just threaten to use, cyber force against an adversary in an attempt to compel them to take a desired action or not take an undesired action.

The DOD defines cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications

networks, computer systems, and embedded processors and controllers" (DOD, 2014, p. 59). As more systems utilize cyberspace and the dependence of militaries grows, the ability to affect other nations and their militaries by cyber methods increases. Coercion, which has been applied in the physical domains in warfare, is applied to the cyber domain in cyber warfare.

Though the Sony Picture example was a nation-state against a private company, cyber coercion is not limited to such a relationship and can be between many kinds of entities. For this thesis, the potential for cyber coercion between two nation-states will be examined.

In his thesis, Daniel Flemming (2014) reviewed various definitions of coercion and demonstrated that for a cyber coercion operation, Schelling's definition best fit. Though Schelling's work was in the context of the Cold War and nuclear war, Flemming walks through the facets of cyber coercion and shows that Schelling's framework of coercion including force and diplomacy, as well as compellence and deterrence, still can aid in understanding how to apply cyber tactics in a coercive manner.

Schelling (2008) provides several examples of how coercion might play out. Two of the best well-known examples are the "prisoner's dilemma" and "game of chicken." In the prisoner's dilemma, it is in the prisoner's advantage to turn on his co-prisoner, for if he does not, but the other does turn on him, he loses. But if he does turn on the other prisoner, even if that prisoner reciprocates, the end result is better. In the game of chicken, if neither car swerves, then both drivers lose. Cyber coercion better fits within the concept of the prisoner's dilemma, given these two concepts of the risks involved in coercion. If two sides both have cyber capabilities, it is an advantage for one to act against the other, for the risk of not using cyber methods is greater. Given this risk, it is stronger for the defense of the United States to explore possible cyber coercive strategies to take advantage of other adversaries.

As implied by the previous definition, coercion can be active or passive. It includes both compellence and deterrence (Schelling, 2008). These two forms of coercion will be further defined.

1. Defining Compellence

Schelling (2008) defines compellence as an active form of coercion. It requires that the coercer take some type of action. Schelling provides an illustration of compelling an enemy to retreat from a battlefield by committing oneself to an action. He gives an example of setting the grass behind the coercer on fire with the wind blowing towards the enemy. This places the coercer in a position where they must act to move to compel the enemy to action.

Compellence places the coercive action in the hands of the coercer. The compellence only goes as long as the coercer is applying the force. This is a defined action, intended to compel the victim to take the desired action. Within the context of cyber, compellence is an applicable form of coercion. The attacker makes a move against the victim with the intention that the victim responds. It is assumed that the attacker must first make a move to coerce the victim. For this thesis, coercion will be viewed from the perspective of compellence. The thesis will propose actions against an adversary that could be taken to coerce the adversary into making a desired move.

2. Defining Deterrence

Schelling defines deterrence as a passive form of coercion (Schelling, 2008). It does not require that the coercer take some type of action. Schelling provides an illustration of placing a car in the way of the adversary's car. If the coercer has placed his car in the way and no longer moves it, it passively serves as a deterrent. The adversary must decide if they desire to crash into the car or to be deterred and not collide.

Within the context of cyber operations, the effectiveness of deterrence remains disputed. Contributing to the argument that deterrence is not effective in

cyberspace is rapidly changing technology, what could be seen as an advantage today might be obsolete tomorrow. Furthermore, many cyber attacks are effective only while the victim is not aware of the vulnerability being exploited. Should a nation-state announce their capability, owners of systems and networks would be able to reinforce against the capability, reducing its effectiveness. This can be contrasted to nuclear weapons where the announcement of a nuclear capability can serve as a deterrent. While the debate continues, the model of nuclear deterrence cannot be applied to cyberspace. Thus, this thesis will focus on cyber coercion as compellence.

B. FACTORS OF CYBER COERCION

To be effective, several factors must be taken into consideration for a cyber coercion operation. Military operations required proper planning before conducting the attack to minimize the risk of failure. Cyber operations are no different. By understanding the factors involved in a cyber coercion operation, the chances for success increase. The planner should have a vision of what is needed to conduct the attack, an understanding of the expected effect of the attack, and an ability to understand the possible responses by the adversary. All of these will better enable military and national decision makers in determining with method, whether cyber or kinetic, to use in achieving the political objective. Those factors to be considered include the goal of the operation, cost of the cyber weapon used, the reversibility of the attack, the reusability of the attack, and the attribution of the attack. These will now be further defined and discussed.

1. Goal

The goal of the cyber coercion operation is to force the adversary to take a desired action or to refrain from taking an undesired action; that is, to be coerced into behaving in a way favorable for the attacker. To achieve this goal, the proper amount of force, or a compelling threat to use such force, must be applied or threatened to a target that will cause enough pain to the victim to seek an end to the pain. This thesis will look in particular at cyber coercion targeting the supply

chain. This was alluded to by the President when he addressed the potential effect a nation-state may have by targeting products and product distribution.

Included with this goal is the desire to not escalate hostilities. Violence for the sake of violence or intentionally provoking another to war is never in the best interest of a coercer, thus escalating hostilities would not be a means of achieving the desired goal. Should a cyber coercive action lead to escalated hostilities, it will be assumed that the operation was unsuccessful.

Another goal would be to minimize collateral effects. As part of the planning process for a cyber coercion operation, possible collateral effects need to also be anticipated. Collateral effects in cyber are defined as “unintentional or incidental effects including, but not limited to, injury or damage to persons or objects that would not be lawful military targets under the circumstances ruling at the time. Include effects on civilian or dual-use computers, networks, information, or infrastructure” (Cartwright, 2010, p. 3). As the Internet is used for both military and civilian purposes, the potential exists that an attack could impact non-military, civilian networks. Though cyber attacks allow for the ability to target a specific host, because of the interconnectedness of the Internet, the risk of an attack on a specific host or network spreading to another one that isn’t targeted exists. An example of the collateral effects that can be caused by a cyber attack was that during the Stuxnet attack, believed to be targeting Iranian nuclear facilities, 40% of the computers infected with the worm were outside of Iran (Farwell & Rohozinski, 2011). Efforts must be taken to understand and minimize the risk of such collateral effects.

The goal of the operation will be the chief driving factor for the attack. If the goal was deemed important enough, an expensive attack could be justified as necessary to achieve the goal. However, some factors such as the legality of the attack could put limits on the operation regardless of the goal.

2. Cost

Cyber weapons, when compared to traditional military weapons, are relatively cheap (Lin, Dam, & Owens, 2009). Cyber attacks can be conducted by individuals using codes that they either generate themselves or can find online. However, for an attack with military precision to achieve a political objective, something needed for a cyber coercion operation, there is an increased cost. The target must first be studied to understand what is to be targeted and how to achieve the goal. This may include reconnaissance on the victim's network to discover vulnerabilities. This requires time and money. Vulnerabilities must then be determined and exploits created.

As vulnerabilities are discovered by computer and software developers, patches and fixes are distributed as generated. While some systems may not be patched and remain vulnerable, zero-day exploits are preferred for an operation to have a high chance of succeeding. Zero-day exploits are exploits in software that are unknown to the developer. The development of these exploits is quite valuable, and they are less common and more expensive for limited use, specialty designed Supervisory Control and Data Acquisition (SCADA) systems. In fact, the U.S. government purchases zero-day exploits from markets (Greenberg, 2012) and it has been claimed that in 2013 the National Security Agency (NSA) spent over $25 million purchasing zero-day exploits (Fung, 2013). However, some program developers will pay if a zero-day exploit is discovered and reported to the developer. For example, the HP's TippingPoint Zero Day Initiative pays thousands of dollars to individuals who discover and disclose an exploit in software. They then work with vendors and developers to develop and release patches to users of the software ("TippingPoint," n.d.). Other markets exist for vulnerabilities as well with brokers who specialize in buying and selling zero-day exploits. Estimates of prices for zero-day exploits based on the software targeted are shown in Table1.

Table 1. Cost of Zero-Day Exploits (from Greenberg, 2012)

Target Software	Cost Range ($ US)
Adobe Reader	5,000 – 30,000
Mac OSX	20,000 – 50,000
Android	30,000 – 60,000
Flash of Java Browser Plug-ins	40,000 – 100,000
Microsoft Word	50,000 – 100,000
Microsoft Windows	60,000 – 120,000
Firefox or Safari	60,000 – 150,000
Chrome or Internet Explorer	80,000 – 200,000
IOS	100,000 – 250,000

Other costs of using exploits exist as well, such as the reverse engineering of code or hardware to find vulnerabilities, development of systems necessary to conduct certain cyber attacks, and the salaries of personnel needed to operate and oversee this process. For example, the fiscal year 2015 DOD budget proposal requested over $5 billion to fund cyber operations across the entire force (DOD, 2014). Comparatively though, these cyber attacks are cheaper than traditional kinetic attacks. Though $5 billion for cyber is significant, the total request by the DOD was nearly $500 billion for the entire department. A single Tomahawk cruise missile costs around $569,000 per missile ("Tomahawk Fact Sheet," 2014) not including the cost of the platform necessary to launch the missile. In determining the method to achieve the effect, such costs will be important to decision makers.

3. Reversibility

It would be desirable for any attacks to be reversible, that is, to be able to undo any damage caused at the termination of hostilities. A reversible cyber attack would be an attack that allows the target to be restored to its original state by the attacker. Such an attack has potential for several reasons. Reversible attacks on mistaken targets such as civilian infrastructure can be terminated and services restored without causing permanent damage and minimizing collateral effects. Collateral damage could be caused by attacking the wrong system or network or by a self-propagating attack, such as a worm, spreading to other

hosts and networks beyond the target. Cyber attacks which do not cause death or injury to people or permanent damage to infrastructure also serve as a more ethical form of fighting (Rowe, 2010).

This also allows an attacker to adjust their attack after the initial attack. In his paper, Rowe offers the option that an attacker could undo portions of an attack if the attack is deemed to be an over-proportionate attack (Rowe, 2010). This is useful in coercion as an attack could be scaled back if it was believed that the attack by the coercer was too strong and would elicit a counter-attack. Rowe also argues that time should be considered in discussing reversibility as some attacks may take a longer time to reverse. He proposes several techniques, one of which is discussed in the thesis, namely cryptographic attacks that encrypt data to prevent its access by the victim.

The ability of the attacker to reverse the damage caused by the attack is an option provided by cyber warfare tactics that is not afforded to commanders by traditional kinetic weapons. With traditional weapons, after hostilities cease, infrastructure damaged or destroyed must be repaired or rebuilt, adding considerable costs and time. But by using reversible attacks, commanders can achieve a desired effect while being able to adjust the damage caused by the attack, a way of minimizing collateral effects after they have been incidentally attacked, and a way of quickly restoring infrastructure after hostilities.

4. Reusability

For this thesis, the reusability of a cyber weapon is defined as the ability to use the same cyber weapon against the same adversary multiple times with the same likelihood of success. Few kinetic weapons have the expectation that once the weapon is used against an adversary, its usefulness is decreased. However, this is true with many cyber weapons since once the vulnerability being exploited is known to the victim, the victim can take steps to lessen the vulnerability and prevent a repeat of the attack.

Because of the problems of reusability, zero-day exploits are very valuable. They increase the likelihood of the success of an attack, since the weakness is not known to the developer or the targeted victim. Bilge and Dumitras (2012) determined that a zero-day attack lasts on average for 312 days before the vulnerability is secured. (These are civilian attacks, however, and a military attack will likely encourage a faster response.) Though the weapon may be rendered ineffective within a few days after use, during the time period it is effective the adversary can enjoy access to an otherwise inaccessible network or system and have access not enjoyed by other potential adversaries. The ability to reuse the attack during this time frame may be enough to achieve the political objective. The lack of reusability does not necessarily impede the effectiveness of the attack for a cyber coercion operation.

If an attack can be used multiple times, its value is increased as the attack can be continually successful without having to utilize additional zero-day exploits. This requires finding a vulnerability or technique that is not easily defended against. If a cyber weapon was created which had reusability even with the full disclosure of the attack, the deterrence portion of coercion would become feasible for cyber coercion. However, given that cyber attacks currently remain defendable once the vulnerability is disclosed, this thesis will look at reusability in terms of compellence.

5. Legality

Legality of warfare in cyberspace remains ill-defined. In his “Advance Questions for Vice Admiral Michael S. Rogers, USN,” the then-nominee for CDRUSCYBERCOM cited this lack of a precise legal definition of warfare in cyberspace as an issue in conducting operations in cyberspace (*Advanced Questions*, 2014). In it, he wrote that while the DOD has a set of criteria for the use of force in cyberspace and is in accordance with Article 2(4) of the United Nations Charter, there remains no international agreement on what constitutes the use of force and one does not appear to be likely in the future. What

constitutes an attack is still not well defined. In the September 2014 Wales Summit declaration, the North Atlantic Treaty Organization (NATO) announced that cyber threats were a growing concern and could be as harmful as conventional attacks, saying “A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis,” which in part highlights the ambiguity of what defines a cyber attack (NATO, 2014, para. 72). As precise DOD criteria are classified, this thesis will use the Tallinn Manual as a start for determining legal status of various cyber operations (Tallinn, 2013). As the legality of cyber warfare is not codified by international laws or treaties, the Tallinn Manual seeks to provide guidance by analogy to current international laws of warfare.

The Tallinn manual is a non-binding study, commissioned by NATO’s Cooperative Cyber Defence Centre of Excellence, on how international law, especially *jus ad bellum*, or the law of conflict management, and *jus in bello*, the law of war, can be applied to cyber warfare. It recognized that some current customary international laws and international norms would apply to cyberspace; however, unique aspects of cyberspace would require additional efforts to fit them to the norms. The Tallinn manual sought to bridge this gap. This thesis will use the Tallinn definitions for what constitutes a cyber attack and discuss how proposed cyber coercion operations could avoid being so viewed in light of the laws of law of armed conflict.

6. Attribution

In May 2014, the DOJ indicted 5 Chinese People’s Liberation Army (PLA) military officers belonging to Unit 61398 of the 3rd on 31 counts of violating U.S. law including the alleged hacking and economic espionage of six U.S. corporations (DOJ, 2014). Attorney General Eric Holder said that this was an important indictment as it was the first time charges had been brought up against hackers acting on behalf of a nation-state. The United States claimed they were

able to attribute illegal cyber activity to not only a specific nation-state, but to specific individuals operating on the other side of the keyboard.

Attribution of attacks is difficult to prove in cyber warfare compared to other domains. In the traditional warfare domains of land, air, and maritime, attribution can be determined by following where the attackers came from or evidence on the ground. For example, during the Iraq War, the United States repeatedly claimed that Iranian forces were involved in improvised explosive attacks on coalition forces, claims which Iran denied. However, the United States was able to produce hard evidence in the form of captured Iranian Revolutionary Guard Corps Qods Force members and weapons with markings traceable to Iranian arms factories (Glanz, 2007). Traceable markings and captured personnel are not usually available in cyber warfare, especially given the use of proxies and forging of IP addresses. Because of this, anonymous attacks are possible, making it difficult for a victim to know who attacked them or prove a possible attacker was the culprit.

In the previously discussed Sony Pictures hack, the FBI claimed they could trace the attack back to North Korea. While the FBI cited national security reasons for not releasing all of the evidence used in the attribution, they did cite three key clues (FBI, 2014). The malware used in the attack showed similarities to previously known malware developed by North Korea, IP addresses hardcoded in the malware had links to known North Korean communications infrastructure, and some of the tools used in the attack were similar to a North Korean cyber attack on South Korea in 2013. This public claim of attribution, however, did not occur until December 19th; nearly a month after the attack was reported to the FBI by Sony. This can be contrasted with the September 11, 2001 attacks on the United States in which by September 20th, President George W. Bush had publicly announced that al Qaeda was behind the attack (Bush, 2001). The difficultly in attribution means that some large cyberattacks have gone unattributed. Despite their high profile, the 2007 cyber attack against Estonia, the 2008 cyber attack against Georgia, and the Stuxnet cyber attack against Iran

have all remained publicly unattributed to a nation-state, beyond unofficial leaks, despite their publicity and supposed connections to various nation-states.

This gives an advantage to attackers who wish to attack a victim with minimal fear of retribution. A nation-state, or even non-nation-state actors, can conduct a cyber attack, achieve the desired damage, and have a reasonable expectation of not having the attack attributed to them and escaping reprisal. This is useful in espionage, when attribution of the activity is not desired. However, what if a nation-state wanted to publicly attribute an attack to themselves? What if a nation-state not only conducted a cyber attack, but publicly announced that they were responsible for it? Intentional attribution is seen by some groups such an Anonymous and the Syrian Electronic Army. However, these are not organized groups and permit anonymity of the individual members. They can publicly claim to be behind an attack to gain notoriety while keeping their identification unknown.

A nation-state might intentionally self-attribute an attack if they were to gain something by it such as political leverage. This could be done by a public announcement, though this would only be supported by the attacker's word and the perceived credibility of the claim. Another possible way might be to embed the attribution within the attack. Such a method could be steganography. Steganography, meaning "covered writing," is hiding of information to prevent detection of even the presence of information (Johnson & Jajoda, 1998). By embedding some type of signature within the attack, the attacker could prove their responsibility for it. By attributing the attack to themselves, the attacker can demonstrate their ability to conduct an attack and could cause the victim to fear another attack, increasing the effectiveness of the attack (Rowe, 2010). It would also clarify what kind of response the coercer desires. It would allow the attacker to better coerce the victim, having demonstrated their ability to apply pain in the form of an attack. Rowe also proposed that cyber attacks containing attribution would be more ethical. This would be akin to soldiers in combat being required to wear the uniform of the nation they are serving. Hare proposed that for

compellence in cyberspace to work, the coercer must have the assurance that the victim has attributed the attack correctly, that the victim understands what action they are being attacked for, and that the victim knows what actions must be taken to end the pain being suffered (2012). Given these arguments, attribution may not only have benefits in coercion, but be required to compel one's adversary.

C. CONCLUSION

Cyber coercion is both a strategy and tactic that is worth the United States exploring and utilizing. Using Schelling's model of prisoner's dilemma, it would put the United States at a disadvantage to not use cyber coercion strategies where appropriate. However, they must be used in terms of the political objectives set out by the United States and in accordance with international laws and norms.

Cyber coercion is active. It places the coercer on the offense. The coercive actions analyzed within these operations will be offensive in nature, meaning that they will not be a cyber posturing by the coercer, but an offensive move, sometimes defined as an attack.

While parallels can be drawn from other domains, cyber coercion operations are unique in their ability to drive effects in terms of cost, reversibility, reusability, and legal status. These unique attributes require a deeper look to understand how cyber coercive strategies might be used by the United States It may be found that in many situations, using cyber coercive actions will be more effective, cheaper, and a cleaner way of fighting than alternative approaches. These same factors, however, also mean that cyber coercion is of strategic significance for our adversaries. Analysis of cyber coercion will help us to understand how our defense cyber capabilities must be placed strategically to minimize the risk of the United States being cyber coerced.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODS OF CYBER ATTACKS TARGETING THE SUPPLY CHAIN

A. TARGETING THE SUPPLY CHAIN

The supply chain that supports a military presents an opportunistic target for cyber coercion operations. The Department of Defense (DOD) in Joint Publication (JP) 1-02, the DOD Dictionary of Military and Associated Terms, defines the supply chain as "the linked activities associated with providing materiel from a raw material stage to an end user as a finished product" (2014, p. 239). This is overseen by supply-chain management, defined as "a cross-functional approach to procuring, producing, and delivering products and services to customers" (Department of Defense, 2014, p. 239). For the militaries, the supply chain is crucial. Military supply chains consist of military and commercial supply, maintenance, and distribution components to provide materiel and logistic services to its military force. The goal, as defined by the DOD in JP 4-09, Distribution Operations, is "to maximize force readiness while optimizing the allocation of limited resources" (2013, p. x). If this component of a military was disrupted, it can drastically negatively affect the ability of a military to wage warfare.

1. Description of the Supply Chain

All supply chains will vary in their structure to support the acquisition of the product. However, there are some commonalities among supply chains. There are five main parts of a typical supply chain: customers, retailers, wholesalers/distributors, manufacturers, and component/raw material suppliers (Chopra & Meindl, 2004). For a military supply chain, the customer is the end user of the product being provided who is using it in support of the objectives of the military. The need generated by the end user and its delivery of the product to the end user are the driving factors of the supply chain. Retailers in the context of the military may include commanders and units which oversee the operations

of the end user. The distributors may include military and commercial distributors who oversee the procurement of the product from the manufacturers and the delivery to the units or end user. The manufacturers include military and commercial producers of the product. The raw-material suppliers provide the necessary material goods to the manufacturers for the manufacturing of the desired product. As supply chains overlap and can be complex, a disruption anywhere within a chain can have cascading effects in denying the ability of the product to be delivered to the end user. If the product targeted is of sufficient critical necessity to the military, it may inhibit the ability of a military to conduct its desired operations.

Military supply chains have traditionally been protected from foreign influence due to critical components being internal to the force. However, with the advent of the Internet, supply chains have grown increasingly dependent on the Internet for communications and coordination between components (Hageman, Harper, Sagan, & Weyman, 2010). The global reach of the Internet creates an opportunity for cyber operations to reach and influence supply-chain operations. As other countries use the Internet to supply their supply chains, this provides opportunities for the cyber forces of the United States to be able to directly affect key aspects of adversarial supply chain operation (Hageman et al., 2010).

2. Reason for Targeting the Supply Chain

As a potential application of cyber coercion is to prevent hostilities from occurring, causing disruption of the supply chain may be a way to prevent a military from fighting. Sun Tzu said, “For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill” (Tzu, 1963, p.77).The ability to disrupt supply chains via cyber attacks as a form of cyber coercion has the ability to fulfill Sun Tzu’s advice, by achieving victory without fighting. It reduces the risk to American service members and the costs associated with combat operations, allowing the United States to exert greater influence in the world at a lower expense.

An example of how a single part of the supply chain can have an effect on combat forces is seen by the United States military's Hellfire missile. The AGM-114 Hellfire missile is an air-to-surface missile that has been used extensively in military operations since being first used in Operation Just Cause. It is the primary antitank weapon system of the U.S. Army and initially designed by the United States as a helicopter launched missile, it has been adapted for use on fixed-wing aircraft, ground units, and shipborne use against a wide-variety of targets ("AGM-114 Hellfire Employment," n.d.; Munoz, 2014). It was used heavily in Operation Desert Shield with an estimated 3,000 to 4,000 Hellfire missiles fired. It has continued to be used in operations in all theaters of combat in the global war on terror such as Afghanistan, Iraq, and Yemen ("AGM-114 Hellfire Employment," n.d.; Mazzetti, Schmitt, & Worth, 2011). However, the supply chain for the Hellfire missile is a weak point. The missile uses a solid-fuel propellant which is made using 1,2,4 butanetriol. The United States is dependent upon one Chinese company for the production of this vital chemical. A disruption in the supply chain for this component could cause the United States to be denied use of this weapon which has become a workhorse for the military (Adams, 2013).

Finding a similar weak point in the supply chain for an adversary's military forces could place their military in a position where, because its supply chain for a vital military weapon system was disrupted, it would not be advantageous for it to begin or continue hostilities. In this way, an operation against the supply chain could prevent combat operations from ever having to take place, achieving political objectives without the risk to the lives of military forces and the expense of fighting a war.

A weakness in a military supply chain affecting operations was seen in the 2003 invasion of Iraq which limited the ability of the U.S. Army to support units with food, ammunition, and needed supplies. This was caused by the communication network for the supply chain being inadequate. Using legacy systems combined with fielding new Radio Frequency Identification (RFID) tracking tags, the Army found it difficult to track supplies once they were in Iraq

and unable to reroute supplies if a unit moved locations. As a result, some units had to resort to pillaging enemy supplies to support their operations (Songini, 2004).While this was not an attack against a supply chain, it shows the affect that degradation in the communication portions of the supply chain can cause. If this were a coordinated attack, the attacker could have targeted and exploited these weaknesses in the communications portion of the supply chain to greatly magnify the effect of the supply chain issues had in delaying or denying the delivery of necessary supplies to military end users.

B. DESCRIPTION OF CYBER ATTACKS

Effective cyber attacks against the supply chain need to disrupt it in a manner that convinces the adversary to not escalate hostilities and to comply with the demands of a coercer. Developing the cyber attacks would require determining the target network, conducting initial reconnaissance on the target, developing the attack, gaining access to the network, maintaining the attack, and terminating the attack.

There are many attacks that can be used to achieve the purpose of cyber coercion on a supply chain. Several types of attacks can be considered given their targeting, including those that target network communications, the manufacturing process, and databases. For each of these attacks, the factors of cyber coercion will be analyzed. The goal of the attack will be reviewed in terms of what success might look like. The cost of the attack will be discussed in terms of development and execution. Given the desirability for any attacks to be reversible, this ability for each attack described will be reviewed. The ability of the attack to be used multiple times will be discussed. In considering the legality of attacks, the Tallinn Manual will be reviewed to consider whether it is a cyber attack which violates a nation’s sovereignty as the primary consideration. While attribution is an important consideration, this will be left for the scenarios in Chapter IV.

1. Targeting Network Communications

Network communications are essential in supply chains. The integration of computer systems within supply chains for data storage and communications has created a dependence of the supply chain on computer networks. The leading reasons computer networks are used within supply chains are for managing demand information, the flow of physical goods, financial information, and ordering (Warren & Hutchinson, 2000). As these are important factors in supply chains, targeting the networks can disrupt the supply chain's ability to deliver products to end users.

Targeting the network would require reconnaissance to determine the services to be denied to drive the desired affect against the adversary. This would then lead to targeting the network and routers to deny access to the intended services.

In targeting networks, routers are a component that could be a force multiplier for an attack, if brought under control. Routers are used to connect networks and to route traffic along a network path to a final destination (Baker, 1995).By targeting a router, one can cause effects against more than just an individual host or hosts, to affect all hosts on a given network and even other networks as traffic transmits across the Internet via routers.

This category of cyber attack methods is quite broad as there are many different attacks that can be used against routers and the networks utilizing these routers. For this analysis, the four broad categories of Internet infrastructure attacks, as categorized by Chakrabarti and Manimara (2002), will be reviewed. These four broad categories are domain name system (DNS) hacking, routing-table poisoning, packet mistreatment, and denial of service (DOS).

a. DNS Hacking

In a DNS attack, the DNS is manipulated with false information to disrupt, redirect, or deny traffic on the network. The DNS serves as the phonebook for the Internet. It is a distributed hierarchical directory which maps fully qualified

domain names to IP addresses, which are used by computers and routers to route network traffic (Chakrabarti & Manimara, 2002). Many local networks include DNS servers which resolve queries from local users.

One potential attack is to poison the DNS by compromising the DNS server and modifying records stored on the server. When a user attempts to go to a website and the DNS query is conducted to resolve the domain name, the IP address returned is the address from the record stored on the server. Modifying this record allows the attacker to redirect traffic to an alternative IP address.

Another potential attack is to spoof a DNS server on a network. By spoofing the DNS server, the attacker is able to control all data distributed in the DNS response to queries given to the server.

The desired outcome of these attacks in a cyber-coercion attack against an adversary's supply chain would include denial of service or redirecting traffic. Denial of service would be achieved by preventing a user from being able to use the DNS to resolve host name to IP address look-ups, potentially denying them the ability to navigate to a desired site providing specific services of the supply chain, such as Websites containing information on inventory or entering in data or communications between systems within the supply chain. Redirecting traffic could be achieved by sending replies that contain a false address of a requested name. The attacker could then create a false service at the specified IP address that mimics the desired service, and could be designed so that the victim uses the service without knowing it has been compromised.

An example of this occurred in a 2014 attack where routers commonly used in small offices or home offices had their DNS settings changed to use a malicious DNS. Hundreds of thousands of routers were observed to have had their DNS settings changed by malicious code inserted using a Cross-Site Request Forgery (CSRF) technique. Though the purpose behind this attack was undetermined, the malicious DNS could direct users to fake Websites in an attempt to steal credentials (Team Cymru's Threat Intelligence Group, 2013).

b. Targeting Router Tables

The routing table is used by routers to determine the path that packets should be forwarded along from the router. Contaminating the information found in this table can cause suboptimal routing, congestion in the network, and denial of service on the network. In a router table poisoning attack, the routing table of a router is intentionally given incorrect information. This table is populated by information that is passed between routers. By compromising a router, an attacker can send false updates to neighbor routers. In an attack on networks using link-state routing protocol, a router under the control of an attacker could advertise a fake link, delete existing links, or change the cost of a link. In networks using distance vector routing protocol, the attack could advertise wrong distance vectors which would be accepted by neighboring routers and propagated throughout the network. By doing so, the attacker can manipulate the path that traffic will take on the network. The traffic could be routed to go through the malicious router, allowing the attack to view or modify the data, or the traffic could be routed in a manner that increases congestion or causes denial of service.

An example of this type of attack occurred in 2008 when the Pakistani government ordered ISP's to block YouTube access. After the government ordered ISPs to censor the website, Pakistan Telecom began advertising a route for IP addresses used by YouTube. This was an attempt to intentionally poison routing tables to reroute traffic destined for YouTube to the provider where the traffic would be dropped. It was used to attempt to prevent people from within Pakistan from accessing the site; however, the false advertisement was made global, resulting in YouTube being blocked worldwide for over two hours. This advertisement by Pakistan Telecom was sent to an upstream ISP, PCCW, where it was advertised to the rest of the Internet al.l traffic to YouTube was then routed to Pakistan Telecom where it was dropped. This continued for nearly two hours before the malicious entry in the routing tables was discovered and blocked by PCCW (RIPE NCC, 2008).

c. Packet Mistreatment Attack

A packet mistreatment attack occurs when a data packet is captured by an attacker and maliciously treated in processing. The packet could be modified with the data being changed to either manipulate data within the supply chain or to prevent data from being transferred across the network. Packets could be duplicated and used in a replay attack against a network. If conducted from a compromised router, the router could be used to drop or misroute the packets. These attacks are harder to detect, but usually less effective than other attacks (Chakrabarti & Manimara, 2002)

d. Denial of Service Attacks

A denial of service (DOS) attack prevents users from using services of a victim's system. This is done by attempting to consume the bandwidth of the victim's network being targeted, consuming CPU resources of the victim's host by forcing the host to process false traffic, and denying access to the victim's services being hosted (Patrikakis, Masikos, & Zouraraki, 2004). Numerous methods are used to create this desired effect. Some common or historic methods include HTTP GET flood, ping flood, "ping of death," Smurf attack, and SYN flood.

An HTTP GET flood attack uses standard HTTP GET method to overwhelm the resources of a server. The GET method requests that the server retrieve and transmit the requested data (Fielding & Reschke, 2014). The attack overwhelms the server resources by flooding the server with these requests. Using the GET method makes the packets used in this attack hard to distinguish from legitimate traffic.

A ping is a network administration utility which sends an Internet Control Message Protocol (ICMP) echo request to a host. The host then responds with an ICMP echo to the source IP address. In a malicious attack, multiple hosts can be used to amplify the attack. In a ping flood attack, multiple hosts send pings to a specific victim, forcing the victim to use resources to respond to the requests.

The desired effect of the attack would be to use enough hosts against the victim to consume the ingoing and outgoing bandwidth of the victim's network and to consume enough CPU cycles in processing the requests to slow down the victim's system.

The "ping of death" attempts to crash IP devices by sending a large packet. In accordance with RFC 791, the maximum size of an IP packet is 65,535 bytes (Postel, 1981). However, the data link layer usually has a smaller maximum size for each frame called the maximum transmission unit (MTU). To allow for this difference, packets are fragmented into smaller packets on the data link layer. Once the fragmented packets are received by the host, they are reconstructed. If a ping request is transmitted with 65508 bytes of data, the packet could be properly fragmented to meet the MTU, and the illegal size of the packet would not be discovered until reconstructed by the receiving victim's host. This could overflow memory buffers and cause undefined behavior by the victim's machine.

A Smurf attack attempts to amplify a ping attack by maliciously using hosts found on a network. A modified ping request is sent to the broadcast network address of the network to be used for the attack. The broadcast network address is an address from which all hosts on a network can receive traffic (Mogul, 1984).The ping request is crafted to include the victim's IP as the source IP address, and then sent by the attacker to the network broadcast address. When each host on the network receives the ping request, it responds with a ping reply to the host identified in the source IP address, which is the victim. The victim is then flooded with ping replies from all the hosts that responded to the ping request. This attack has been mitigated by recommendations to router settings in RFC 2644 (Senie, 1999).

Another example of a DOS attack is a SYN Flood. A SYN Flood occurs by not completing the TCP three-way handshake. When establishing a TCP connection, the client transmits a SYN message to the host. The host then responds with a SYN-ACK message. The client completes the connection

establishment by sending an ACK message. The vulnerability exists when a client sends the initial SYN message, the host replies with the SYN-ACK message, but then the client never transmits an ACK message. This creates a half-open connection. The client will often have a time-out associated with these connections to terminate the half-open connection if it does not complete within a certain amount of time. By continually creating many of these half-open connections using different, spoofed source IP addresses, an attacker can consume client resources resulting in additional incoming connections being denied ("TCP SYN Flooding," 2000). Publicized in a hacker magazine called Phrack in 1996, this attack was used against Panix, an Internet Service Provider (ISP) in New York. The attack targeted various servers including Web and mail, causing outages which prevented legitimate traffic from accessing the servers (Eddy, 2007; Patrikakis, Masikos, & Zouraraki, 2004).Since then, mitigations have been recommended to limit the threat of SYN flooding, but the attack still demonstrates the effect of a simple DOS attack can have.

These types of attacks can be amplified by using more than one host to attack in a distributed denial of service (DDOS). A DDOS attack is used to prevent the victim from doing their desired work (Internet Architecture Board, 2006). The related idea of a botnet could be useful to control potentially thousands of hosts to attack a specific host with. A botnet is a collection of compromised computers which can be controlled by an attacker for malicious purposes, such as spam email or denial of service attacks. For example, one botnet in 2008 called Srizbi was estimated to contain around 315,000 computers and could send 60 billion emails per day (Keizer, 2008). Using a distributed attack also makes the attack harder to deter. With the attack coming from potentially thousands of vectors, it is difficult for network administrators to identify the source of the attack to mitigate. This increases the potential for the attack to be successful and have a longer duration.

A botnet is typically created by compromising hosts by injecting malware into the host. The host then runs the malware and joins the botnet. The infected

hosts on the botnet communicate with a controller that provides the commands for the intended activity of the botnet. The controller then provides maintenance and upgrades to the botnet as necessary (Zhu, Lu, Chen, Fu, Roberts, & Han, 2008).

The duration of a DDOS attack will vary based on how long the attack is staged by the attacker and how long it takes for the victim to observe and respond to the attack. Akamai, a company that specializes in minimizing global DDOS attacks, estimated that DDOS attacks in quarter four of 2014 had an average duration of 29 hours, up from 22 hours the previous quarter (Akamai, 2015).

e. Costs

Network attacks are quite cheap. These types of attacks are commonplace as they can be conducted by anyone with access to the Internet and the code necessary to conduct such attacks is readily available.

Creating a botnet requires time, resources, and exploits. To create a botnet for which the attacker had full control of would require purchasing, modifying, controlling, and maintaining thousands or millions of hosts. To create a botnet using hosts found on the Internet would require an exploit which could compromise a host. Kits for purchase online exist to help facilitate the creating of a botnet, lowering the barrier to entry (Wilson, 2010). Given the effort needed to create and maintain a botnet and the prevalence of botnets already in existence, it might be desirable to use botnets already in existence. Some hacker groups already rent out their botnets. Computer security company Damballa found that the typical rate for renting a DDOS botnet was around $200 for 10,000 hosts in a botnet per day (Ollman, 2009). This amount varied based on the size of the botnet rented and location of the hosts. Another possible way of creating a botnet is using JavaScript embedded on Websites using an online advertising service (Greene, 2013). Researchers at White Hat Labs were able to create a million-bot botnet by placing malicious JavaScript within ads. They then paid for the ads to

be seen on the Internet. While a user's browser was on the website with the malicious ad, it was executing the JavaScript which targeted a Web server to attempt to overwhelm it. The test was successful and the cost of the botnet was about $150.

f. Reversibility

While terminating this attack is easy, reversing any effects of it are not reversible. Terminating the attack will allow the network to recover, but any damage caused by the network being down cannot be expected to be recoverable, including communications that were attempted. Depending on the network affected, this can have various levels of affect.

g. Reusability

Using this attack does reveal what method was used. The victim could be able to harden their network to deny the coercer from reusing this type of attack. IP addresses utilized may now be blocked from accessing the target network. If a botnet was utilized, discovery of the botnet may lead to its compromise. Given that no network is 'DDOS proof,' other DDOS methods could be used, but the level of attack needed to cause the denial-of-service is elevated.

h. Legality

The legality of a network attack is not conclusive. Article 2(4) of the U.N. Charter prohibits nation-states from using or threatening to use force against other states during peacetime. In applying this to cyberspace, Rule 10 of the Tallinn Manual prohibits cyber operations which would be considered a threat or use of force against a nation-state (Schmitt, 46). However, the definition of the "use of force" is ambiguous. Rule 11 attempts to define the use of force, comparing the size and effect of the attack to a non-cyber operation (Schmitt, 2013). As mentioned in the discussion of this rule, a DOS attack is not likely to be classified as a use of force, thus not an act of war. However, the potential for a victim to classify it as a use of force exists, given the ambiguity of the definition of

use of force. Due to the potential for severe unintended consequences which could elevate the perspective of the global community that the attack constitutes the use of force, caution must be taken by the attacker to ensure collateral damage is minimized.

When states are at war, the use of force and conduct of armed attacks is governed by the law of war. To apply this to cyberspace, the Tallinn Manual defines a cyber attack as “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects” (Schmitt, 2013, p. 92). Although attacks on a network are not normally physically destructive, they can be. Moreover, they may have unintended physical consequences. An attack on a network such as a network support air-traffic control could cause destruction and potential loss of life.

The use of rented botnets would likely violate Rule 32, the prohibition on attacking civilians given the process of acquiring the bots by maliciously taking over computer hosts (Schmitt, 2013). Though the hosts used to make up a botnet are not known, it can be assumed that computers used by civilians make up a significant portion of bots (hosts) in a botnet and this would constitute targeting civilian objects. These civilian objects would then be used by the military for an attack without user consent and opening the civilian object up to reprisal attacks.

2. Targeting the Manufacturing Process

The manufacturing process of the supply chain also poses a potential target for cyber attacks involved in cyber coercion. Military forces depend on technical parts and equipment which must be manufactured. This may include parts manufactured by either military controlled production plants or by contracted manufactures.

Two parts of the manufacturing process serve as potential targets for a cyber coercion operation, the industrial-control systems that control the

equipment used in manufacturing and the end product. The manufacturing portion of the supply chain is relevant not just before hostilities, but also during hostilities. This justifies targeting of the manufacturing process

a. Targeting SCADA Systems

Industrial-control systems used to remotely control manufacturing equipment are an opportunity for a cyber-coercion attack to disrupt the manufacturing part of the supply chain. SCADA systems control remote operations of and data flow from control devises used in the manufacturing process. Many of these systems connect to the Internet or use wireless protocols for network communications, allowing access for an attacker. Zhu, Joseph, and Sastry (2011) provide a taxonomy of attacks against SCADA systems divided into three groups: cyber attacks on hardware, cyber attacks on software, and attacks on the communication stack.

A cyber attack on the hardware of the SCADA system could involve an attacker gaining access to a device and maliciously changing its set points or manipulating operator displays to prevent their observation of equipment malfunction. This could cause the system to not behave as expected by causing devices to fail or causing an operator to be misinformed of the current operating status of the equipment. An example of an attack like this occurred in 2000 when a disgruntled employee attacked the Maroochy, Queensland, Australia sewage equipment SCADA system (Abrams & Weiss, 2008). The employee attacked the system 46 times, manipulating the equipment, disabling alarms, and causing over 200,000 gallons of raw sewage to be released into ponds and streams. The attacker launched his attack from his vehicle which he had loaded with the necessary radio equipment. This attack highlights the vulnerability of SCADA systems and shows the effect of such an attack by even an individual attacker operating with knowledge of the targeted system and equipment to exploit the system.

A cyber attack on software could target the software necessary for the SCADA system to meet its functionality demands. Targeting the software can have an effect on databases, technical data needed for control algorithms, and business functions. Many control applications were written in the C programming language which contains several known vulnerabilities that could serve as vectors into the SCADA software systems such as buffer overflows. VxWorks is a popular embedded operating system. Because it operates all applications as kernel tasks, all tasks are run with the highest privileges. This could allow a malicious user to gain privileged access to other programs on the device. Another software target is the database. Gaining access to the software could allow the attacker to modify or delete order or product information (Warren & Hutchinson, 2000)

A successful targeting of SCADA systems occurred with the Stuxnet attack, revealed in 2010 in use against Iran. The Stuxnet worm was designed to target a Siemens SCADA computer system which was used in the Iranian nuclear-fuel enrichment program (Hounshell, 2010). It is believed that Stuxnet was written to target the Iranian nuclear program, as 60% of the infected computers were discovered in Iran (McMillan, 2010).The worm exploited Windows vulnerabilities by means of four zero-day attacks to gain access. The program then determined if the infected computer contained the Siemens software being targeted. If the computer did not contain of the targeted software, the program became inert. If it did contain Simatic WinCC, the worm would attempt to reach back to a command and control server to download the latest version of the code. It then targeted the Siemens SCADA systems via additional zero-day attacks. The program monitored the targeted system and used the intelligence gathered to gain control of centrifuges used in the nuclear-fuel enrichment processes. The speed of the centrifuges was varied by the program, causing the centrifuges to physically break. To confuse the operators of the industrial system, the program feed false information to the controllers, preventing the operators from knowing of any issues until the centrifuge was

broken (Kushner, 2013). One of the ways that the Stuxnet worm propagated was via thumb drives (McMillan, 2010). This enabled the worm to gain access to networks not accessible to the Internet.

Though the full extent of the Stuxnet virus has not been reported, it is believed that it may have destroyed around 20% of the centrifuges used by Iran in their enrichment program (Kelley, 2013).It is also possible that Stuxnet destroyed around 1,000 centrifuges at the enrichment plant in Natanz, Iran (Albright, Brannan, & Warlond, 2010). This attack demonstrated the damage that a cyber attack can cause by targeting SCADA systems. Cyber security expert Ralph Langer said Stuxnet "changed global military strategy in the 21st century" (Kelley, 2013).

b. Targeting End Products

Targeting the products developed in the manufacturing process would involve embedding an exploit either through software, firmware, or hardware in the end product which would give at attacker control of the product to enable disrupting or denying its use in future operations. For example, if such an exploit was embedded in the control system of a missile could allow an attacker to control the flight of the missile after launch, diverting it from its intended target or possibly sending it to a new target. In a cyber-coercion attack, demonstrating control over an adversary's weapons would deny the adversary the use of such weapons.

Such an exploit could be embedded as a backdoor, allowing the attacker to have future access to the product, or as a logic bomb. A logic bomb is malicious code which is designed to sabotage operations when certain conditions are met. In the example of the missile, a logic bomb could execute when a certain condition was met such as being fired, achieving a certain altitude, or being given certain coordinates for targeting. An example of a logic bomb attack occurred in a 2013 attack against South Korean banks and broadcasting companies. The logic bomb was propagated via an email phishing scheme. It

was written to be executed at a specific time and simultaneously deleted hard drives and master boot records of at least three banks and two broadcasting companies (Zetter, 2013).

While an attack on the end product of the manufacturing process can prevent the product from operating as designed, it is important for the attacker to control when and where the attack occurs to have the best effect in cyber coercion. It also allows the attacker to conduct an attack which may be reversible. Should the conditions of the cyber-coercion operation be met favorably for the attacker, the embedded code could be removed or revealed to allow the compromised product to return to its initial, uncompromised condition.

As certain weapons and other pieces of equipment are essential to the operations of the military, critical items are stockpiled by the military supply system to ensure availability when needed. To ensure this attack could be used, it would be even more effective to attach the backdoor during the manufacturing process to be able to compromise all products in the inventory. This would require access to the manufacturing process before hostilities began. Access could be achieved using other cyber methods or by gaining physical access to the manufacturing equipment.

A successful attack would require that the malicious code or other exploit not be discovered. Discovery would not only compromise the ability to conduct cyber coercion, but also potentially cause escalations in hostilities as the victim may desire to take punitive action against the attacker if it is possible to identify them (something quite difficult). However, the risk of discovery may be low because of the prevalence of counterfeit parts, since a number have been found in U.S. military systems. A 2012 study by the U.S. Government Accountability Office (GAO) found that counterfeit parts are readily available from vendors used to procure military-grade electronic parts. Further, a 2012 Report of the Committee on Armed Service of the United States Senate reported that a study conducted in 2009 and 2010 found over 1,800 cases of counterfeit parts, totaling over 1,000,000 affected parts. Further, case studies presented in the report show

that many of the counterfeit cases included cases where the part was observed to not match expected physical characteristics, but was still used, and the counterfeit part was only removed after parts failed. So malicious code has a reasonable chance of not being detected as long as the equipment maintains its normal working condition until the attack is executed.

c. Costs

Attacks on the supply china can be expensive. Attacks on SCADA systems exploit vulnerabilities in computer hosts and the SCADA software which are only known to a few people, and they also require access to the limited-access networks where these specialized hosts and software reside.

Initial reconnaissance of the facility to be targeted is required to determine the computer hosts and SCADA software used. Vulnerabilities must then be determined and exploits created. As vulnerabilities are discovered by computer and software developers, patches and fixes are distributed as generated. While some systems may not be patched and remain vulnerable, zero-day exploits are preferred for an operation to have a high chance of succeeding.

If the target was a more specialized or less common system such as Siemens SCADA systems, then the cost increases. In fact, the U.S. government runs a research facility, the SCADA Security Development Laboratory, which analyzes SCADA systems for vulnerabilities (“SCADA History,” 2012). The additional research necessary elevates the cost of an attack. One estimate of Stuxnet says that it cost over $10,000,000 to develop. Estimates of the time it would take to develop are between one and five man-years for programmers (Stark, 2011).

Similarly, attacks on end products also have a high cost of entry. The cost of development is potentially higher than SCADA systems as the attacker must develop exploits for the computers within the manufacturing plant, the control systems of the equipment used to manufacture the product, or the product itself, all of which require solving specialized challenges. The cost of this type of attack

could be comparable to the previously discussed zero-day exploits. Reuter's Joseph Menn claimed that the NSA paid RSA, a network and computer security company, $10 million to set an NSA developed algorithm, called Dual Elliptic Curve, as the default algorithm used to generate random numbers used in the BSafe cryptography software (2013). It was alleged that this random number generator has a backdoor in it, allowing the NSA to gain access to data encrypted using the software. Although this was a deal struck with the company producing the product, not an operation carried out against the product, it gives a good indication of, if true, the amount of money a government is willing to pay to gain access to end products.

These costs are greater than for a denial-of-service attack, but cause a greater effect on the victim's ability to conduct military operations and have a longer duration.

d. Reversibility

An attack which targets the software of the SCADA or end product and has not damaged any physical property is easy to reverse, if the coercer reveals how the necessary steps. If the attack is activated so that it actually damages or destroys physical property, this is not reversible. If the attack manipulated or damage hardware beyond repair, this would require the hardware be replaced. Further, other effects may have to be dealt with. The Maroochy water service attack caused environmental effects. A representative from the Australian Environmental Protection Agency said, "Marine life died, the creek water turned black and the stench was unbearable for residents" (Abrams & Weiss, 2008, p. 1). Such consequences must be considered for an attack where physical effects are possible.

e. Reusability

Discovery of an attack on the manufacturing process may lead victim to review how the coercer was able to access their systems. This may lead to changes in policy that make it harder to access the system as before. For

example, if thumb drives were used to gain access into an air gapped network, the USB ports of the network might be administratively turned off to prevent their use. Other vulnerabilities that were used to access the target might also be discovered and mitigated. If discovered, this attack is hard to reuse.

f. Legality

Given the Tallinn Manual definition of cyber attacks, the legality of attacks during war on the manufacturing process of a supply chain is dependent upon its target and its intended effect. Attacks on SCADA systems can cause physical destruction and potential loss of life. In the two examples, the Maroochy attack and the Stuxnet attack, both qualify as attacks if placed in the context of international conflict as they both caused damage or destruction. If an attack on the SCADA system caused the system to simply not work correctly without damaging equipment and could be reversed without damaging the equipment and without other physical effects, the attack would be less likely to meet the threshold of a cyber attack. If this attack was conducted outside a time of war, it would likely be considered an illegal attack if the attack was designed to manipulate the controls within a military industry, especially if the attack caused physical effects. However, discovery of the attack prior to activation would not likely be classified as use of force as no force has taken place, merely the ability to use force. Further, the attack before activation may be indistinguishable from espionage.

Attacks on SCADA systems also have a risk of collateral damage in that some SCADA systems used for military production purposes are also used for civilian purposes. This was demonstrated by the spread of the Stuxnet virus to targets that were not likely the intended target. As the virus sought to propagate itself and sought to exploit specific Siemens SCADA software, the virus would spread to computers that were not the intended target of the attacker; over 40% of the computers infected by Stuxnet were outside of the most probable target of Iran (McMillan, 2010). So an attack on SCADA systems could spread beyond its

intended target to critical infrastructure such as electrical grids. Such spreading of an attack could be prohibited under rule 51 of the Tallinn Manual, “A cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited” (Schmitt, 2013, p. 132).

Having the capability built into the product of being able to take control of it would not in itself be a cyber attack. It would cross the threshold of cyber attack when the code was activated and the product no longer operated as expected. In the example given of gaining control of a missile, this would occur when the missile did not operate as expected. If the attack was targeted against something not as disposable or used more than one time, such as a backdoor embedded into a computer chip, and was reversible in that the code could be removed or deactivated, it would be less likely to be recognized as a cyber attack as the operation could be designed to simply cause the system to not work for a short time without physical damage to equipment.

3. Targeting Databases

Databases are collections of data, organized to enable processing by users or systems. Some databases are extremely valuable to the owner because of the information they contain and the purpose the data is processed. If these valuable databases can be located, targeted, and rendered inaccessible to the adversary, a significant advantage may be gained by hindering the process or system the database supports.

a. Encryption Attack Against Databases

Databases are used extensively in supply chain management to track orders, monitor inventory, oversee transportation, and do numerous other data tracking tasks. Their importance and extensive use provide a good target for cyber coercion. By removing access to a database, an attacker can affect all

parts of a supply chain, including ordering, manufacturing, transportation, and distribution.

A potential attack against a database would be to use reversible cryptography. A reversible cryptography attack encrypts selected adversary data, preventing the adversary from having access to the encrypted data, then decrypts the data at the end of hostilities (Rowe, 2010).This type of attack does not modify or delete the data, but only prevents the adversary from being able to use it This type of attack could be accomplished using public-key cryptography, an asymmetric-key cryptographic procedure which uses two keys, a public key and a private key. Data encrypted with one key can be decrypted with the other key. In practice, the public key is available publicly and anyone can encrypt data which only the older of the private key can decrypt. This is commonly used in digital signatures, key transport, and key agreement (Kuhn, Hu, Polk, & Chang, 2001). A public key could be delivered by some malicious code to an adversary's database. When activated, the code would use the public key to encrypt the data, rendering the data inaccessible until decrypted using the private key. A message could then be relayed to the adversary that their data will be decrypted once the desired conditions are met. This reversible attack allows the desired effect of the cyber attack to be achieved without destruction of data.

An advantage of using asymmetric keys is that should the key embedded in the system be discovered, it would not decrypt the data. A disadvantage compared to symmetric keys is that encryption by public key schemes is slower (Kuhn et al., 2001).This could be overcome by creating a symmetric key for the encryption process, and then the symmetric key could be encrypted using the public key. The encrypted key could then be stored until the attacker decrypted it using the private key. This would avoid the potential loss of the attack should the malicious code be discovered during the encryption process.

The code could be delivered by gaining access to the system using a vulnerability discovered during the reconnaissance phase or by targeting an unsuspecting system user using spam emails containing the malicious code. For

systems not accessible to the Internet, targeting system users with infected thumb drives and other removable media could allow access.

Launching the attack could be done by having the malicious code call back to the attacker for instructions or by inserting a logic bomb to control when the attack would occur. Using the logic bomb has the advantage of not being dependent upon communications between the attacker and the victim's database after the code has been inserted. However, it also has the added risk of not being able to be controlled once the code is inserted. The attacker may not be able to prevent the attack from occurring once he has inserted the code into the database system, even if earlier steps in coercion have succeeded in effecting a change in the adversary.

In September 2013 this type of attack was used in a program called CryptoLocker (Jarvis, 2013). This malware was ransomware, malware which exploits system vulnerabilities to gain access and encrypt data files to prevent a user from using or accessing their files unless a ransom payment is paid. This often involves a transfer of funds using online accounts or digital currency (Luo & Liao, 2009). CryptoLocker was initially disseminated using spam email containing malicious attachments with the CryptoLocker executable. Later, it was distributed using the peer-to-peer Gameover Zeus malware. Spam email would be sent to a user containing a malicious attachment that contained code which would download Upatre malware, which would then download and execute Gameover Zeus, which would download CryptoLocker onto the user's computer. Once on the computer, the malware would attempt to reach back to a command-and-control server. Once the connection was established, the server would generate a 2048-bit RSA key pair and pass the public key to the malware. The malware would then encrypt targeted files. CryptoLocker was written to target files based on their extension. A window would appear on the user's screen informing them that their files had been encrypted and providing instructions on how to pay the ransom to restore the files, usually on the order of several hundred dollars. A timeline was given for paying the ransom before the private key was to be

destroyed. If the ransom was paid, the program then decrypted the files, restoring them to the victim (Abrams, 2013). By April 2014, over 234,000 computers were estimated to have been infected by CryptoLocker and tens of millions had been paid in ransom (DOJ, 2014). CryptoLocker has demonstrated that an encryption attack is possible, and by the amount of ransom paid, that it has a great effect on the victims.

This type of attack requires extensive reconnaissance prior to initiating. The attacker must target a database of enough significance that the victim is unwilling to continue hostilities and will acquiesce to the demands of the attacker. The attacker must also determine if backup copies of the database are kept, or else the victim could restore the database, rendering the attack considerably less serious. If backup copies are kept on the network, these backups must also be removed either by deletion or encryption to ensure the database could not be restored. If tape backups are created, the attacker could target the backup process prior to the attack on the database to have all recent backups be corrupted. The attacker might also replicate the attack several times, increasing the amount of data lost since the last successful backup prior to the attack until enough data is lost that the attack on the database is effective.

b. Costs

This type of attack is not expensive once access to a target system has been achieved. Encryption commonly occurs with data transmission and storage on networks, and key pairs can be generated using readily available software. MalwareMustDie, a security research group, found that a malware similar to CryptoLocker called Prison Locker was being sold online for $100 (unixfreaxjp, 2014). The biggest cost would come in determining the database or databases to encrypt and gaining access to them using known or discovered vulnerabilities.

c. Reversibility

This attack is reversible, if the coercer gives over the private key, or if the coercer maintains or is given access to the target database. The encryption will

not manipulate the data, but only prevent its use without the key. Thus, this attack is completely reversible.

d. Reusability

The encryption attack itself is reusable. Even if the private key is revealed, if a secure encryption scheme is used, the attack can be repeated using a new public-private key pair. However, access to the database may be denied. To reuse this attack, a new method of accessing the database will be required.

e. Legality

As the encryption is reversible and does not damage the data, this operation does not meet the threshold of a cyber attack. However, if the operation occurred while the two nation-states were not at war, because the operation targets the cyber infrastructure of another state, it would be a violation of sovereignty as defined in rule 3 of the Tallinn Manual, “any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty.” (Schmitt, 2013, p. 29)

C. CONCLUSION

This chapter surveyed attack methods that could be used to target portions of the supply chain. The target chosen could be based on what is believed to be best to coerce the adversary to take no further hostile action, and also could be based on what parts are accessible. Targets such as communications within a supply chain may be targeted cheaply, but with a short duration. Targets within a manufacturing process incur a higher cost, but with a potential greater effect. Database targets provide a cheap and effective method of denying an adversary access to data. It is important that the method find a balance between providing enough pain to the adversary to discourage them from continuing their action without applying so much that escalation occurs.

A favorable characteristic of many of these attacks is reversibility. This is something that cyber warfare can provide to commanders as a tool for achieving

the goals of a military objective without the destructive nature of kinetic weapons. Though many of these tools are reversible, those that are not still could produce less destruction to achieve the same goal as kinetic weapons. These tools do not have to operate independently and can be used together with other tools and the threat of further kinetic force to drive the effect of denying the adversary access to his supply chain without the destroying his infrastructure.

IV. SCENARIO

A. INTRODUCTION

In this chapter, three scenarios will be presented and analyzed, each using one of three cyber-coercion attacks previously described in Chapter III. The scenarios show the threat of additional or continual attacks, including both cyber or kinetic, against various types of adversaries can encourage de-escalation. By having cyber coercive attacks available as options to military commanders and national decision makers, additional opportunities short of conventional warfare exist to further U.S. interests. The application of such strategy exists in situations where U.S. action is desired, but there is little public or political support for full scale military operations.

Cyber operations in support of military objectives hold advantages over other military operations. While cyber operations can cause physical destruction and even lead to loss of life, the cost of achieving the objectives of the operation can be much less than having to mobilize, deploy, and support combat soldiers. It also could allow for military operations without soldiers being placed in harm's way. Having a lower cost and less risk to military forces in achieving the same objective can lead to greater support for cyber operations verses conventional military operations. Further, a nation-state might have an obligation by the principle of unnecessary risk and harm to use cyber methods over kinetic methods with the same capabilities for legal purposes (Denning & Strawser, 2014).

This exercise is important. Before conducting an operation, or when determining what actions other nations might take, the military reviews possible outcomes to determine what might be the most likely outcome and the most dangerous outcome. This enables decision makers to understand the risks and gains for each possible operation. As mentioned previously by CDRUSCYBERCOM, U.S. cyber forces remain in the early stages of being able

to do this. Cyber forces need to be able to present the expected outcomes for different cyber operations, including those launched by the United States, those launched against the United States, and those launched between other nations. This chapter seeks to further this endeavor.

B. SCENARIO BACKGROUND

For these scenarios, an encryption attack, a distributed denial-of-service attack, and a SCADA attack, will be discussed in different situations. The method will be described including the type of attack, the target of the attack, and the attribution, termination, and possible responses by the adversary. The measure of effectiveness of a coercive attack will be the degree to which the attack leads to escalating the conflict or not. As the goal is to enable the coercer to further its international interests while preventing conflicts from escalating, if the method is likely lead to escalation of cyber or kinetic weapons by either side, it will be considered not successful.

For the scenarios, these attacks will be launched by the same coercer. This coercer is a modern nation with a highly capable military with world-wide reach and a sophisticated cyber capability, including both offensive and defensive abilities. These scenarios will also include discussion on possible effects if the United States was the subject of the coercive operation.

The purpose of coercion is to use the threat of force to compel your adversary to take a desired action or to deter the adversary from taking an undesired action. Sometimes a show of force is necessary to demonstrate the ability of the coercer to conduct an action and to show the credibility of the threat of further force. This may be something more of a demonstration such as a carrier strike group transiting the Strait of Hormuz, a massing of military forces such as Operation Paul Bunyan where a large contingent of ground and air elements were massed near the Korean Demilitarized Zone in support of a tree clearing operation, or an actual attack, such as Commodore Decatur’s capture of the Dey of Algeria’s flagship in the Second Barbary War. All these actions

intended to communicate the message that the United States has the ability to cause pain to the adversary.

With cyber weapons, it is not as easy to conduct a show of force in comparison to a Strait of Hormuz transit. With nuclear weapons, testing may not only serve to gain knowledge of the use of the weapon, but also sends a signal to would be adversaries that your country has such ability. This demonstration is not possible with cyber weapons. Once a cyber weapon is used, the adversary has the opportunity to reverse engineer the attack to strength their cyber defenses to prevent the attack from working again. Something more similar to Commodore Decatur's action is required, where an actual cyber attack is made with the threat of more cyber attacks or even kinetic attacks to follow if the desired action is not taken. As such, the risk of escalation is increased. Each method analyzed in the scenarios will be treated as a show of force, where the coercer demonstrates their ability to apply pain to the adversary with the attack, while the threat for more attacks lingers if action is not taken.

For the scenarios, the important factors previously discussed for cyber coercion will be discussed, as appropriate. The reversibility and reusability of the attack will be discussed, along with its implications. The legality of the coercive operation will be reviewed using the Tallinn Manual as the basis. Additionally, both self-attributed and non-attributed attacks will be analyzed. Given that the need for attribution still remains disputed in cyberwarfare, these scenarios will include attacks launched using both perspectives.

C. SCENARIO ONE

The first scenario is a cyber coercion operation conducted in which supply-chain databases are encrypted using public keys against an adversary who has modern cyber capabilities with positive attribution. The scenario is against an adversary who is posturing to invade or has begun an invasion of a neighboring country.

1. Attack Description

The adversary in this scenario is assumed to be a modern country with advanced cyber capabilities including defensive and offensive capabilities. Their military is modern with a global reach on a par with the coercer military. This country utilizes the Internet for their supply chain in similar ways the coercer military does, for communications, supporting automation of manufacturing processes, procurement, managing inventory, overseeing transportation, scheduling deliveries, and processing orders.

For this scenario, assume the adversary is postured or is currently invading a neighboring nation with whom the coercer is allied or partnered with. This scenario also assumes that because of this alliance and the hostile situation, the coercing nation-state is supporting its ally in its right to use armed force for self-defense against an armed attack. A cyber operation could serve to coerce the adversary into taking an action favorable to the coercer. This action might be withdrawing troops from a neighboring country or to standing down from posturing for a potential attack. The goal of the attack is to disrupt the supply-chain process of the adversary, in conjunction with the posturing of coercer military forces, in a manner which causes the adversary to not escalate the situation.

To be effective, the cyber attack would need to target databases of significant value to the supply chain. The databases need to be essential so that without the information contained within, the supply chain is greatly hampered. The databases cannot be easily replaced and must be an essential component of the supply chain. Prior reconnaissance could enable the coercer to determine the appropriate target; good potential targets include databases containing order information, inventory, or coordination of transportation and delivery of supplies. Targeting essential supplies such as military food, fuel, and ammunition could increase the effectiveness of the attack. Denying the ability of the adversary to access the data within these databases could severely hinder their ability to

conduct military operations by disrupting the ability of the adversary to deliver supplies to their troops in forward operating areas.

Access to the database could be done during the reconnaissance phase. Given the adversary has advanced defensive capabilities, the adversary could detect that the coercer has accessed their networks. This could be seen by the adversary as routine penetration or espionage. While the adversary may react by bolstering security, espionage is not considered an act of war and would not be expected to lead to an escalation of hostilities, given how often these types of occurrences have become (Lewis, 2010). This cyber weapon could be left installed on the target database prior to the decision to execute. This could be activated by a logic bomb on a certain date or by accessing via a backdoor. A logic bomb would be similar to an attack against South Korea seen in March 2013 which embedded itself onto banking and broadcasting companies systems and was activated on a specific date and time (Zetter, 2013). Further, if the encryption could use public-key encryption, if the payload of the cyber weapon were compromised, only the public key would be exposed so the attack could not be analyzed until deployed.

Upon activation of the attack, the database would become encrypted using the public key which only the private key could decrypt. The adversary will have lost all ability to access the encrypted information of the database. At this time, the coercer could expose that they were behind the attack. Attribution would help further the message that the adversary forces need to be withdrawn or face further action by coercer forces. The cyber attack would cripple the adversary from being able to conduct operations and the associated threat of force, both additional encryption attacks and kinetic force, would seek to persuade the adversary to not escalate the conflict.

2. Possible Outcomes

At this point, the adversary could acquiesce to coercer demands and maintain the status quo, respond with cyber attacks against the coercer, or escalate the situation and engage in kinetic action with coercer forces.

The first possible outcome is that the adversary acquiesces to coercer demands. They could signal to the coercer that they do not intend to continue their operations and either completely withdraw their forces or seek a negotiated settlement between the adversary, the coercer, and the neighboring country. Driving the adversary to the negotiating table would achieve the objects of this scenario. This would be the most beneficial outcome to the coercer. Upon the adversary demonstrating their compliance with coercer demands, the database would be decrypted. The database would be returned to use by the adversary with no permanent damage done.

At this point, the adversary made be able to return to their previous aggressive state. Since the attack was only temporary, the supply chain and military forces return to the same condition as they were before the database was attacked. The adversary would likely also determine how the database was accessed and harden the security of the networks to prevent the exploit was being used again. It can be assumed that any exploits left behind on the databases would be discovered and additional backups of the database created. These actions by the adversary would make it difficult to redeploy the same attack using the same vulnerability. However, there are likely many vulnerabilities, and since the encryption process itself is still secure, the attack could be replicated against other databases using these new vulnerabilities. So though the exact attack may not be possible, the same style of attack remains possible. This threat of further similar attacks serves to compel the adversary to compile with coercer demands. The adversary becomes aware of a cyber capability of the coercer, knows that the coercer is willing to use the capability, and knows the effect the capability has. This will serve to encourage the adversary to not return to their previous aggressive state.

The second possible course of action by the adversary is to respond to the coercer attack by launching their own cyber attacks. This would not require that the adversary assume the attack met the threshold of a cyber attack or an act of war. Capable cyber forces likely have advance persistent threats (APT) within potential adversarial networks. APT's are cyber operations which seek to gain and hold access to a network. These can be used for intelligence gathering or as footholds for launching cyber attacks. A cyber force may access a network, plant malicious code within the network, and wait to execute the code until the desired time. For example, the Mandiant report (Mandiant, 2013) revealed that Chinese military forces have APT's within U.S. networks which are used to conduct cyber espionage, resulting in hundreds of terabytes of data stolen from 141 different organizations in 20 different industrial sectors. Given the extensive access to networks by this APT, the possibility exists that malicious codes and cyber weapons may be planted on these networks, waiting for future offensive use. Viewing the encryption attack against their databases as requiring a response, the victim country may begin similar attacks against coercer networks, both military and commercial networks, using their APT's as starting places. This could lead to an escalation of cyber warfare between the coercer and the target country.

The third possibility is that the target country responds to the cyber operation with non-cyber military action against the coercer. Their justification for escalating the hostilities would be that the encryption attack violated their sovereignty and given the potentially already heated situation between the coercer and the targeted country, this would be the cause for war. This is not likely since the operation doesn't meet the threshold for a cyber attack, and the international community would not view it as a proportional response. It would be the most dangerous outcome, and could occur if the target country has been subjected to a series of repeated setbacks with a common origin country.

3. Scenario Conclusions

The outcome of this scenario is that the adversary in unable to access their data and acquiesces to the coercers demands. However, there is a risk that the adversary responds with non-cyber effects or in kind to the encryption attack with their own cyber counterattacks. The ability of a nation-state to resort to non-cyber responses to cyber attacks has been argued by the United States. CDRUSCRYBERCOM said regarding the U.S. response to the hack on Sony Pictures, “Merely because something happens to us in the cyber arena, doesn’t mean that our response has to be focused in the cyber arena” (Frizell, 2015, para. 6). Nation-states using cyber coercion methods must be ready to deal with responses outside the cyber domain. Coercer cyber defenses must be ready to handle attacks against our own networks. Many states target non-government commercial networks for industrial espionage. These may serve as potential targets for cyber counterattacks during a conflict. The coercer must be prepared for a cyber conflict to include systems and networks that will have a direct effect on the civilian population of the coercer.

The strength of this attack lies in the strength of the encryption and the difficulty of restoring the attacked resources from backup. If the encryption scheme was compromised, the attack would lose most of its effectiveness; strong encryption schemes must be used, and the private key must be securely stored to prevent being compromised. Encryption also serves to make the attack reversible, restoring the database at the end of hostilities to its antebellum state. The effectiveness of an adversary’s backup methods will also be important, and can vary considerably; intelligence can provide some clues. An added strength of this attack is causing the adversary to lose confidence in their other military databases. Having demonstrated the ability to gain access and encrypt a database, the adversary could lose confidence that their other databases have not been accessed and manipulated by the coercer.

This attack is very promising, but requires extensive reconnaissance and development and has the risk of causing an escalation of cyber warfare between

the coercer and the adversarial state. Use against a less capable nation would reduce this threat. Even against a more capable nation, the operation may cause the adversary to lose confidence in other military databases. This lack of faith in their own data may serve to be advantageous for the coercer in placing the adversary in a position where they are uncertain of their ability to conduct operations.

4. Susceptibility of the United States to This Coercion

An encryption attack against the United States could cause similar debilitation. As this attack has already been seen in the wild in the form of CryptoLocker, administrators of databases need to ensure that their databases are up-to-date in security and regular backups are made, including backups that are not connected to the network.

D. SCENARIO TWO

The second scenario is a cyber-coercion operation in which supply-chain management communications are disrupted using distributed denial-of-service tactics against an adversary who has lacks modern cyber capabilities, without attributing the source of the attack. The scenario further assumes an adversary led by a repressive regime who is actively putting down a populist uprising which is seeking to overthrow the regime. The coercing nation is seeking to end the actions of the regime, though without U.N. authorization for military operations. The scenario will analyze the possible outcomes of a cyber-coercion operation in response to the coercer demonstrating this capability.

1. Attack Description

The adversary in this scenario is a developing country with limited defensive and offensive cyber capabilities. Their military is moderately capable with a regional reach. Assume this country uses the Internet less for their supply chain than the coercer military does, but still uses the Internet for

communications, supporting automation of manufacturing processes, procurement, managing inventory, overseeing transportation, scheduling deliveries, and processing orders. Being a developing country, they likely have contracts with other countries to provide weapons and supplies necessary for their military.

Targeting the distribution and transportation portion of the supply chain could potentially weaken the military of the regime. For instance in Syria during the current civil war, President Bashar al-Assad's forces suffered low morale due to logistical issues hampering supplying forces fuel and food (Harding, 2012). This led to defections of forces and fears of the regime's imminent fall. If a cyber attack could cause denial of logistical services, confidence of the military forces could be shaken as their forces would be placed at a tactical disadvantage.

There are several considerations in planning a denial-of-service attack like this. These include collateral damage, the legal status of the target, and the legal status of the attack.

Denial-of-service attacks on networks can cause collateral damage on other networks. As the Internet is a shared medium for communication, the excess traffic generated in the attack may disrupt traffic and cause unintended services to be degraded or denied. If the nation-states were at war, the target of the DDOS attack would be legal as it is a military objective, assuming it means other requirements such as necessary and proportionate (Schmitt, 2013). Further, this type of cyber operation does not rise to the level of a cyber attack (Schmitt, 2013). However, since the nation-states are not at war, this legally falls under the more ambiguous legal status discussed in Chapter III. As discussed, a DDOS attacks is not likely to be considered a use of force. Given this, caution must be taken regarding collateral damage as critical systems could be affected. If an operation was to take down critical infrastructure such as the electrical grid or controls for a hydroelectric dam, physical damage could occur. Such unintended consequences may serve as justification for the victim to retaliate against the coercer and elevate the operation to the level of an attack.

If this attack occurred while in a war, since governments use private companies to support military supply chains, this attack could target a non-military network and include civilian objects. However, it falls within the accepted exception to civilian targeting in the Geneva Conventions for industries contributing to military preparedness. Since the target is a valid military objective, it would still be a valid target for a cyber attack (Schmitt, 2013). This could possibly provide justification of the type of attack for the coercer, if the attack was attributed to them, though the coercer would still need to justify the attack in the first place. However, if the country has contracts with larger, more modern countries to support its military supply chain, targeting must be careful to not target systems of the supporting country. An attack on the supporting country could lead escalating hostilities between the coercer and the supporting country, creating a larger international diplomatic issue than before, if the attack was attributed.

This attack would be expected to be limited in duration. As previously discussed in Chapter III, the average distributed denial-of-service attack lasts only 29 hours. Once the attack is detected, mitigations can be put in place by the victim to block attacking IP addresses and to absorb the volume of the attack on the target servers. Cloud-computing companies such as Akamai provide resources for customers which are able to absorb DDOS attacks and other defensive mechanisms to mitigate the effect (“The Challenge,” n.d.). This greatly reduces the ability for the attack to be used again. A military observing an essential network being susceptible to a denial- of-service attack would work to strengthen the defense of not only this network, but other similar networks. While the attack may be able to be used again against other networks in the short term, it is not likely that this type of attack would have long effectiveness.

This attack could be difficult to publicly attribute to the coercer. Given that this attack does not rise to the Tallinn Manual level of a cyber attack, not attributing itself to the attack may allow the coercer to incur the benefits of the attack with freedom from attribution if desired. Non-attribution also may be

desirable if a non-state actor is acting on behalf of a nation-state. A nation-state might provide a non-state actor with the technology or tools necessary for the desired operation. If a nation-state was to hire or encourage a non-state hacker group to conduct an operation against the target state, they may be able to deny involvement in the operation. However, though the operation is conducted by the non-state actor, the support provided by the nation-state may violate international law (Schmitt, 2013).

2. Possible outcomes

There are several possible outcomes based on how the victim nation responses. These include responding to the cyber operation by acceding to the desired behavior, responding with cyber attacks against the coercer, or no major change to their operations.

If successful, the cyber operation can cause a shortage of key supplies such as fuel for military forces in the target country. This fuel shortage places it at a tactical disadvantage, and this coupled with the fear of another DDOS attack and pressure from the coercer and the international community to cease its military response to the populist uprising, may cause the victim country to back down. They may see their current position as not favorable for further military actions. Given their lack of will to continue military operations, they may have negotiations with opposition leaders and the military situation could be diffused.

Though this may be the most favorable outcome for the coercer, this outcome is not likely based solely on a DDOS attack. Previous DDOS attacks, while having short term effects on the targets, have been mere annoyances. They are not likely to be reproducible given the hardening of to the target networks and services after the initial assault. Their impact is minimal beyond the frustrations caused by denial of services.

If the adversary determines or believes that the attack came from the coercer, a military kinetic response is not expected. Since the attack did not meet the requirement of a cyber attack, there would not be justification for a traditional

military response. However, they country may respond with cyber warfare of their own. Even if the target country does not have extensive cyber offensive capabilities, similar countries have been able to launch cyber attacks against coercers on soft targets. During the Syrian civil war, the Syrian Electronic Army attacked Western Websites by redirecting site traffic to false sites (Newcomb, 2015). During the conflict against ISIL, Western social media accounts were compromised by hacking passwords, including the Twitter account of U.S. Central Command (Lamothe, 2015). While these attacks were not significant, they did garnish national attention. Iran has also launched denial-of-service attacks against U.S. banking Websites (Gorman & Barnes, 2014). Iran was also able to launch an attack against a military target, the Navy Marine Corps Intranet (NMCI). In 2013, it was reported that Iran had infiltrated the unclassified network and conducted intelligence gathering (Gorman & Barnes, 2014); this attack took several months to fully recover from.

A third possibility is that the attack has minimal effect on the target country since many DOS attacks can be recovered from quickly. During the 2008 cyber attack against Georgia, Georgian sites which were taken down by denial-of-service attacks could be restored on servers that were not subject to the attack including commercial servers such as Google or servers in other countries (Moses, 2008). The attack was certainly a disruption, but the effectiveness is hard to judge as it coincided with ground operations. In 2007, a large attack against Estonian Websites was launched due to Estonia moving a World War II Soviet memorial, and the attacks lasted for over a week; NATO and other international support was sought to secure Estonian networks, but the statue was still moved (“Estonian fines man,” 2008; Joubert, 2013). These denial-of-service attacks, while annoying, did not serve to meet their objective.

3. Scenario Conclusions

This type of attack could be quite limited in its effect against an adversary as described. Due to the limited duration, it is not likely to be able to stop a

military. Thus, this type of attack would be mostly ineffective for a cyber coercion operation.

It may be better if targeted in specific tactical situations to support operations. For example, if coercer forces launch a DDOS attack on an air-defense network to prevent nodes from being able to communicate, air defenses could be temporarily compromised, allowing coercer aircraft to safely enter a denied area. Also, as seen in the DDOS attacks against Estonia and Georgia, civilian morale can suffer when civilian infrastructure such as financial institutions is denied. This ability to erode civilian morale by targeting civilian infrastructure likely extends to targeting social media. Countries dealing with uprisings, such as Syria, have turned off the Internet within their country, possible to disrupt protestors utilizing social media (Thompson, 2013). By disrupting the ability of people to use social media, the morale of the civilian base could drop. This targeting of civilian morale does not by itself constitute a cyber attack (Schmitt, 2013). However, explicitly targeting civilian infrastructure with cyber weapons would be against international law.

4. Susceptibility of the United States to This Coercion

This type of attack is already seen in the United States, both against military and commercial networks. The networks operated by the DOD are routinely attacked and this includes DDOS attacks (Chandler & Loyless, 2009). A recent DOD study showed that DOD network services are vulnerable to a DDOS attack (OSD, 2015). While susceptible, given previous DDOS attacks, the duration of the attacks is likely to be short given the ability to move services to other servers, block attacking hosts, and absorb DDOS attacks.

E. SCENARIO THREE

The third scenario is a cyber coercion operation in which the manufacturing portion of the supply chain is targeted to embed a backdoor into a weapon system which allows the coercer to control the weapon. This will be targeted against an adversary who has modern cyber capabilities with positive

attribution. The scenario assumes an adversary is currently engaged in combat operations against the coercer or a partner nation.

1. Attack Description

The adversary in this scenario is assumed to be a modern country with advanced cyber defensive and offensive capabilities. Their military is modern with a global reach. This country has modern weapon systems which are manufactured in modern industrial facilities. These facilities use networks for controlling SCADA equipment and other automated processes and often are unknowingly connected to the Internet (Klick & Marzin, 2013).

The operation could serve to coerce the adversary into ceasing combat operations by denying the adversary use of their weapons system. During combat operations, the coercer would force the weapon system to not act as expected, either by not functioning or by not being able to strike its intended target. The coercer would take credit for the weapon system's failure. This would place the adversary at a tactical disadvantage, force the adversary to cease use of the weapon system or reconfigure it, and spread fear that other weapon systems are also compromised.

The attack would need to target a weapon system of significant value like a missile system. If the coercer were able to embed a backdoor or a logic bomb into the guidance system of the missile that could be accessed at the time the missile is fired, the coercer could direct where the missile goes, potentially missing its target or hitting a target chosen by the coercer By demonstrating control of the missile, the adversary would lose confidence in the weapon. The weapon would need to be taken out of use until the exploit is discovered and removed. If the adversary has many missiles that are dispersed, this could be a significant task.

For this weapon system, the coercer may already have kinetic capabilities of achieving the same end results of denying the adversary use of the weapon. However, by conducting this cyber compromise of the weapon, the coercer can

drive greater effects than just denying the use of the missile. The cyber compromise allows for the coercer to manipulate use of the weapon regardless of its location and the location of coercer defense systems. It also drives fear into the adversary that other weapon systems may be compromised, and significant efforts may be exerted to look for possible vulnerabilities in other systems. Since weapons are stockpiled by militaries, this exploit would need to be implanted potentially years before it might be used.

Access to the manufacturing process could allow access to the programming of the weapon system to achieve the goal. Though many SCADA systems are intended to not be accessible to the Internet, researchers from the Freie Universität Berlin have discovered that many SCADA systems have interfaces to the Internet (Klick & Marzin, 2013). Even if the SCADA system does not have an Internet access point, as in the Stuxnet attack, thumb drives and other removable data storage devices can gain access to isolated networks via willing or ignorant users (Sale, 2012). Accessing the process when the computer components are programmed and integrated into the weapon system would allow manipulating the code to inject a backdoor or logic bomb, allowing the coercer future access to the weapon or causing the weapon to not operate as expected. Another potential access point for injecting the vulnerability may be during maintenance of the weapon.

There is potential that the exploit is discovered before it is activated to disable the weapon. Although it may do nothing to the weapon until activated, there is potential dispute between the coercer and the adversary as to whether the operation constitutes a cyber attack or not. The experts utilized for the Tallinn Manual were split if such operations met the threshold of an attack during a time of war. One argument is that the damage necessary for an attack does not occur until the exploit is activated. The other argument, explained by analogy within the Tallinn Manual, is “there is an attack whenever a person is directly endangered by a mine laid” (p. 94). Given that the classification of this operation is ambiguous, the risk must be understood prior to executing it. If it was discovered

before the two nation-states entered a state of war, it would not be likely that this would be considered a use of force. Further, discovery of the exploit might not enable to victim to determine if the exploit was intended to control the weapon system or cyber espionage.

Upon activation of the attack, it would be desirable that the coercer expose that they were behind the attack. In this situation, attribution would be important to strengthen the coercer's message that the adversary forces need to cease hostilities as their trust in their weapon systems diminishes. The fear of further weapons failing and being placed in a tactically unfavorable position against the coercer or coercer-partner forces will be an incentive.

2. Possible Outcomes

The adversary has several reactions they may take after the coercer has demonstrated the ability to control their weapon system in combat. The adversary could acquiesce to coercer demands, change weapons they are using, or isolate and remove the exploit from the compromised weapon system and continue operations.

If the adversary acquiesces to coercer demands, they could signal to the coercer that they do not intend to continue their operations and either completely withdraw their forces or seek a negotiated settlement between the adversary and the coercer and the coercer partner nation. Driving the adversary to the negotiating table would achieve the objects of this scenario. Upon the adversary demonstrating their compliance with coercer demands, the exploit could be removed as part of the negotiations. Allowing for the possibility of being able to use the exploit again allows for great leverage by the coercer

A second possible course of action by the adversary is to change weapons. Since this is a capable military force, they have weapon systems that are likely not of the same effectiveness as the weapon system that has been compromised, but can be used for similar effects. By changing their weapon system, they could be able to continue their combat operations with

uncompromised weapons. This could be negative for the coercer if they do not have countermeasures for the alternate weapon systems, but if the coercer does have countermeasures and wants to encourage use of weapons that they have countermeasures for, this may be a very favorable outcome. By choosing which weapon systems are exploited, the coercer could steer an adversary to a weapon system of the coercer's desire. In this case, cyber coercion is not realized, but a tactical advantage is gained.

The third possibility is that the target country finds the exploits, removes the exploits, and places the weapon system back into service. This may be possible if an original exploit-free copy is available as backup. This would be the most dangerous outcome for the coercer. It returns the conflict to its condition before the exploit was activated. Despite years of development, implanting the exploit, and activating the exploit, the advantage gained by the coercer is lost. Further, the adversary may reverse-engineer the exploit and reuse it against the other states.

3. Scenario Three Conclusion

The desired outcome of this scenario is that the adversary coerces to the demands of the coercer as the adversary is unable to use the targeted weapon system. If the exploit is placed in multiple systems, a greater effect is gained. More weapons are taken out of service and the confidence of the adversary in their own weapons diminished. If enough weapon systems are taken out by this cyber operation, or if the enemy is placed in a severe enough tactical disadvantage, the cyber operation may serve to coerce the adversary into meeting coercer demands. However, there is the possibility that the adversary resorts to another weapon system. Being able to drive the adversary to use an alternative weapon system for which countermeasures exist could turn this into a favorable outcome.

The adversary may seek to increase their defenses of their SCADA systems and the software installation process of weapon systems. But unless the

exploit is found and removed, though the level of effort needed to infiltrate networks is increased, the original vulnerability remains and the attack can be used again in the future. This will serve as deterrence of future actions against the coercer as future adversaries will fear that they too may have exploited weapon systems.

This type of attack requires early planning, extensive reconnaissance and development, and has the risk of being discovered. It must be of sufficient value and size to achieve the desired coercion effect. The success of this attack is found in undermining the adversary's trust in their own weapon systems. Demonstrating control of one weapon system with a strategic message that other systems may be compromised puts the belief in the minds of the military forces, as well as the civilians, that their weapon systems cannot be trusted. This erosion of trust in the weapon systems may have a tremendous effect. This effect is seen in terrorist attacks which spread fear among a populace that though the attacks are few and risks of death or injury are low compared to normal daily activities, that the populaces trust in their government to protect them in undermined.

4. Susceptibility of the United States to This Coercion

This type of attack could be used against the United States. Many of the weapon systems used by the United States use precision guidance, and if that portion of the weapon were compromised, the weapon will be rendered inoperable. Further, as previously discussed in Chapter 3, many of the parts used by the U.S. military are manufactured overseas and the danger of compromised parts is significant. Further tightening quality of control for parts developed by the U.S. military's supply chains is necessary to reduce the risk of compromised parts being placed into weapon systems. The security of industrial manufacturing needs to be reviewed as significant numbers of SCADA systems, including those in the United States, were discovered to be accessible on the

Internet. This is important for SCADA systems used in critical infrastructure such as water and electrical systems.

F. ANALYSIS

From these three scenarios, several insights are possible regarding the target of the attack, the size of the attack, and the ability for the attack to be reutilized.

The target of the attack must be sufficient to place the adversary at a tactical disadvantage for the attack to be effective. This helps further the coercive effect of the attack by including the threat of effective military force against the adversary. This is expected to be achieved in an encryption or SCADA system attack. In the case of the DDOS attack, this is not likely given the expected short duration of the attack and the lack of achieving a threat beyond mere annoyance.

The size of the attack must be sufficient to allow for the tactical disadvantage to be gained and to demonstrate the effectiveness of the attack. If the SCADA attack targeting a weapon system only took out one weapon, the effect is minimized and the threat message is not effective. However, the uncertainty about whether additional weapon systems have been compromised can place fear in the adversary that is advantageous for the coercer. If the DDOS attack was large enough to cause the services used by civilians to be disrupted, it may amplify the attack and might cause the morale of the civilians to turn against the regime (or perhaps against the coercer). However, it would be illegal to target civilian objects (Schmitt, 2013).

Finally, the ability to reattack the adversary greatly increases the coercive effect of the attack. This is a weakness of both the DDOS attack and the supply-chains attacks since adversaries can take measures quickly to ensure they are not repeated, at least in the same way. Note also that the encryption attack has a shorter turnaround time for development and redeployment.

Based on this analysis, the DDOS attack is not viable for a coercive strategy, while the encryption and supply-chain attacks are promising coercive strategies. All three may be useful for disrupting communications and supporting tactical combat operations, but the DDOS attack is not likely to create a big enough effect to force the adversary to acquiesce to coercion. The supply-chain attack targeting a weapon system can have the desired effect, but requires extensive planning and execution prior to combat operations. Furthermore, it risks escalating hostilities if discovered during a time of peace prior to execution. The encryption attack shows the most promise by achieving the desired effect, being reproducible, and minimizes damage to the system by being reversible. But it does require a certain degree of access to the target systems.

THIS PAGE INTENTIONALLY LEFT BLANK

V. FINDINGS AND FUTURE WORK

A. FINDINGS

Targeting the supply chains of an adversarial military with cyber weapons can cripple the military to the point of being coerced to some desired activity of the coercer. This is advantageous to the United States in implementing its foreign policy and could be used by an adversary against the United States as well.

The effect of coercion depends on the target of the attack and the type of the attack. Three targets within supply chains and three types of attacks were analyzed for their usefulness in a cyber coercion operation. These attacks had different advantages and disadvantages, however, some methods appear to be better suited than others for the task of coercing and adversary.

The target must be significant enough to create enough pain when that portion is degraded in its operation, although this is difficult to judge. Regardless of the type of attack used, if it can successfully affect an essential link in the supply chain enough to cause sufficient pain to the victim, it can achieve the goal. Of the targets examined, targeting SCADA systems used in the manufacturing of and use of key weapon systems had the greatest effect. Targeting these components could render a military unable to continue its operations, at least without drastically adjusting their plans.

The coercive attack must be sustained and reusable. If an attack can be easily terminated by the victim, it may be reduced to only being an annoyance, as with denial-of-service attacks: Though cheap to launch, their endurance is limited and many tactics can reduce their threat. Encryption attacks hold promise in being sustained and reusable. These attacks are hard to recover from without access to the key if restoration from backup is difficult. This allows the coercer to sustain the attack as long as desired. This attack can be reusable as using unique keys allows each attack to have some variation, though exploits to gain access to each system are still necessary and a new one may be needed for

each system. Reusability of an attack seems to be a premium in cyber warfare, so an attack which can be used and still maintains its future effectiveness is advantageous.

Reversibility is a unique attribute of certain cyber attacks that gives cyber coercion operations additional flexibility and aids negotiations. While the necessary level of pain against the victim may be achieved without reversible attacks, having the ability to quickly reverse attacks and restore the data targeted could encourage negotiations to end the conflict and reduce the chance of escalating hostilities. Since reversible attacks could be low-scale while still maintaining their pressure, the coercer could reduce an attack to a level where the justification for the victim to respond with violence or kinetic options would be poor. Instead of crossing a line in the sand and forcing the victim to make a response, it allows the coercer to cross the line and force the victim to make a response, while allowing the coercer the option of restoring the line. Finally, should the victim acquiesce to the coercers demands, restoring services and databases targeted to their pre-conflict status is cheaper and easier than if violent coercive methods were used.

Cyber warfare can be best accomplished technically by complete anonymity. However, to coerce an adversary, revealing the coercer is valuable. A victim may be more likely to be coerced by a nation-state than by a non-nation-state, given the platitude that democracies refuse to negotiate with terrorists. Revealing the source of the coercion does expose the coercer to retribution, but may be necessary to make clear the coercer's demands and encourage the victim into giving in.

B. FURTHER RESEARCH

Further research in cyber coercion should study the value of attribution in cyber warfare and the value of economic sanctions versus cyber coercion. Understanding the effect of attribution is important for decision makers to understand the risks and advantages of self-attributing an attack. To coerce and

demand something from someone, the person who is being coerced must usually know who is making the demand. However, previous attacks should be studied to see if they could have been more effective by the aggressor nation-state publicly attributing the attack.

Economic sanctions and cyber coercion should be compared for effectiveness in achieving similar political objectives Economic sanctions are currently seen as a diplomatic method that should be used prior to military options. However, their effectiveness is not certain and the reasons are not well understood (Morgan & Schwebach, 1997). Additionally, sanctions can harm civilians in the target country more than to the government targeted (Weiss, 1999). However, cyber coercion has its own disadvantages discussed earlier.

C. CONCLUSION

Cyber coercion, though currently limited as a foreign-policy tool, has promise of being able to manipulate an adversary to cause sufficient pain for the adversary to acquiesce to the coercer's demand without escalating hostilities. Attacks on essential portions of supply chains, such as SCADA systems in the manufacturing portion or key databases, and encryption attacks, show the most promise of preventing the adversary from continuing unfavorable operations, while allowing the coercer to sustain the attack and reuse it in the future. The United States should explore the use of cyber coercion as part of its foreign policy as a supplement to other kinds of coercion, to continue furthering American influence in the world while reducing its military footprint. However, given the widespread availability of cyber weapons and the growing dependency of cyberspace for military applications, the United States must be prepared for these tactics to be used against itself. Failure to adequately appreciate the potential for these operations in the hands of adversaries could place the United States in a weakened defense position.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abrams, L. (2014, October 31). CryptoLocker ransomware information guide and FAQ. Retrieved from http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

Abrams, M., & Weiss, J. (2008). *Malicious control system cyber security attack case study–Maroochy Water Services, Australia*. McLean, VA: The MITRE Corporation.

Adams, J. (2013). *Remaking American security: Supply chain vulnerabilities & national security risks across the U.S. defense industrial base.* Retrieved from https://s.bsd.net/aamweb/main/page/file/63cb7de914604943ba_oxm6be590.pdf

Advance questions for Vice Admiral Michael S. Rogers, USN: Hearing before the Senate Armed Services Committee. 113th Cong, (2014).

AGM-114 Hellfire employment. (n.d.) Retrieved from http://www.globalsecurity.org/military/systems/munitions/agm-114-employ.htm

Akamai. (2015). *Akamai's state of the internet*. *Q4 2014.* 1(2). Retrieved from http://www.stateoftheinternet.com/downloads/pdfs/2014-Internet-security-report-q4.pdf

Albright, D., Brannan, P., & Walrond, C. (2010). *Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant?*. Institute for Science and International Security.

Baker, F. (1995). *RFC 1812: Requirements for IP version 4*. Internet Engineering Task Force, Fremont, CA.

Bilge, L., & Dumitras, T. (2012, October). Before we knew it: an empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 833–844). ACM.

Bradner, E. (2014, December 24). Obama: North Korea's hack was not war, but 'cybervandalism.' *Cable News Network*. Retrieved from http://www.cnn.com

Bush, G. W. (2001, September). Address to Joint Session of U.S. Congress. Presented at U.S. Congress, Washington, D.C.

Cartwright, J. E. (2010, November). *Joint terminology for Cyberspace Operations* [Memorandum]. Washington, D.C.: Department of Defense.

Chakrabarti, A., & Manimaran, G. (2002). Internet infrastructure security: A taxonomy. *IEEE Network*, 16(6), 13–21.

The challenge: Safeguarding against DDOS attacks. (n.d.). Retrieved from http://www.akamai.com/html/solutions/protect-against-ddos-attacks.html

Chandler, S., & Loyless, J. (2009). PKI: The DOD's critical supporting infrastructure for information assurance. *Crosstalk: The Journal of Defense Software Engineering*, 22(7), 10–15.

Chopra, S. & Meindl P. (2004). Supply chain management (2nd ed). Upper Saddle River, NJ: Pearson Prentice Hall.

Denning, D. E., & Strawser, B.J. (2014). Moral cyber weapons. In M. Taddeo & L. Floridi (Eds.), *The Ethics of Information Warfare* (pp. 85–103). New York, NY: Springer.

Department of Defense. (2013, December 19). Distribution operations (Joint Publication 4–09). Washington, D.C.

Department of Defense. (2014, March). United States Department of Defense fiscal year 2015 budget request. Washington, D.C.

Department of Defense. (2014, December 15). Department of Defense dictionary of military and associated terms (Joint Publication 1–02). Washington, D.C.

Department of Justice, Office of Public Affairs. (2014, May 19). U.S. charges five chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage [Press Release]. Retrieved from http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Eddy, W. (2007). *RFC 4987: TCP SYN flooding attacks and common mitigations*. Internet Engineering Task Force, Fremont, CA.

Estonia fines man for "cyber war." (2008, January 25*). British Broadcasting Corporation*. Retrieved from http://www.bbc.com/news

Farwell, J.P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival: Global Politics and Strategy,* 53(1), 23–40. doi: 10.1080/00396338.2011.555586

Federal Bureau of Investigation. (2014, December 19). Update on Sony investigation [Press Release]. Retrieved from http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

Fielding, R., & Reschke, J. (2014). *RFC 7231: Hypertext transfer protocol (HTTP/1.1): Semantics and content*. Internet Engineering Task Force, Fremont, CA.

Flemming, D. (2014). Offense-In-Depth: an analysis of cyber coercion. Master's thesis, Naval Postgraduate School, Monterey, CA.

Freedman, L. (1998). *Strategic coercion concepts and cases*. New York, NY: Oxford University Press.

Frizell, S. (2015, January 8). NSA director on Sony hack: 'The entire world is watching.' *Time*. Retrieved from http://time.com

Fung, B. (2013, August 31). The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities. *The Washington Post*. Retrieved from http://www.washingtonpost.com

General Accounting Office (GAO). (2012). DOD supply chain: suspect counterfeit parts can be found on internet purchasing platforms. Retrieved from http://gao.gov/assets/590/588736.pdf.

Gifis, S. H. (1991). *Law dictionary* (3rd ed.). New York, NY: Barron's.

Glanz, J. (2007, February 12). U.S. says arms link Iranians to Iraqi Shiites. *The New York Times*. Retrieved from http://www.nytimes.com

Gorman, S., & Barnes, J. E. (2014, February 18). Iranian hacking to test NSA nominee Michael Rogers. *The Wall Street Journal*. Retrieved from http://www.wsj.com

Greenberg, A. (2012). Shopping for zero-days: a price list for hackers' secret software exploits. *Forbes*. Retrieved from http://www.forbes.com

Greene, T. (2013, August 1). Black Hat: How to create a massive DDoS botnet using cheap online ads. *Network World*. Retrieved from http://www.networkworld.com

Hageman, H., Harper, I., Sagan, P. M., & Weyman, A. (2010). *Cyber threats to national security: countering challenges to the global supply Chain.* Comprehensive National Cybersecurity Initiative International Inc, Virginia, 11.

Hare, F. (2012, June). The significance of attribution to cyberspace coercion: A political perspective. In *Cyber Conflict (CYCON), 2012 4th International Conference on* (pp. 1–15). IEEE.

Harding L. (2012, July 27). Syrian army supply crisis has regime on brink of collapse, say defectors. *The Guardian*. Retrieved from http://www.theguardian.com

Healey, Jason. (2014, July 30). Commentary: Cyber deterrence is working. *Defense News*. Retrieved from http://www.defensenews.com

Hounshell, B. (2010, September 27). 6 mysteries about Stuxnet. *Foreign Policy*. Retrieved from http://foreignpolicy.com

Inquiry into counterfeit electronic parts in the Department Of Defense supply chain: Report of the Committee on Armed Services United States Senate. 112th Cong, (2012).

The interview: A guide to the cyber attack on Hollywood. (2014, December 29). *British Broadcasting Corporation*. Retrieved from http://www.bbc.com/news

Jarvis, K. (2013). Cryptoware ransomware. Retrieved from http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, 31(2), 26–34.

Joubert, V. (2012). *Five years After Estonia's cyber attacks: Lessons learned for NATO?.* NATO Defense College, Research Division.

Keizer, G. (2008, April 9). Top botnets control 1M hijacked computers. *Computer World*. Retrieved from http://www.computerworld.com/article/2536378/security0/top-botnets-control-1m-hijacked-computers.html.

Kelley, M. B. (2013, November 20). The Stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought. *Business Insider*. Retrieved from http://www.businessinsider.com

Klick, J., & Marzin, D. (2013, May). Find them, bind them – industrial control systems (ICS) on the Internet. Presented at PHDays , Moscow, Russia.

Kuhn, D. R., Hu, V. C., Polk, W. T., & Chang, S. (2001). *Introduction to public key technology and the federal PKI infrastructure*. National Institute of Standards and Technology, Gaithersburg, MD.

Kushner, D. (2013). The real story of Stuxnet. *IEEE Spectrum*, 50(3), 48–53.

Lamothe, D. (2015, January 12). U.S. military social media accounts apparently hacked by Islamic State sympathizers. *The Washington Post*. Retrieved from http://www.washingtonpost.com

Lewis, J. A. (2010). The cyber war has not begun. *Center for Strategic and International Studies.*

Lin, H. S., Dam, K. W., & Owens, W. A. (Eds.). (2009). *Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities.* National Academies Press.

Luo, X., & Liao, Q. (2009). Ransomware: A new cyber hijacking threat to enterprises. *Handbook of research on information security and assurance*, 1–6.

Lynn, W. J. III. (2010). Defending a new domain: The Pentagon's cyberstrategy. *Foreign Affairs*. 89(5), 97–108.

Mandiant. (2013). *APT1: Exposing one of China's cyber espionage units*. Retrieved from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Mazzetti, M., Schmitt, E., & Worth, R. (2011, September 30). Two-year manhunt led to killing of Awlaki in Yemen. *The New York Times*. Retrieved from http://www.nytimes.com.

McMillian, R. (2010, July 23). Iran was prime target of SCADA worm. *Computer World*. Retrieved from http://www.computerworld.com

Menn, J. (2013, December 20). Exclusive: Secret contract tied NSA and security industry pioneer. *Reuters*. Retrieved from http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220

Mogul, J. C. (1984). *RFC 919: Broadcasting Internet datagrams*. Internet Engineering Task Force, Fremont, CA.

Morgan, T. C., & Schwebach, V. L. (1997). Fools suffer gladly: the use of economic sanctions in international crises. *International Studies Quarterly*, 41, 27–50.

Moses, A. (2008, August 12). Georgian websites forced offline in 'cyber war.' *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au

Mulrine, A. (2011, June 9). CIA Chief Leon Panetta: The next Pearl Harbor could be a cyberattack. *The Christian Science Monitor*. Retrieved from http://www.csmonitor.com

Mulrine, A. (2013, July 12). Rebuilding Iraq: Final report card on U.S. efforts highlights massive waste. *The Christian Science Monitor*. Retrieved from http://www.csmonitor.com

Munoz, C. (2014, January 14). SNA 2014: Navy won't rule out Army Longbow Hellfire for LCS. USNI News. Retrieved from http://news.usni.org.

NATO. (2014, September 5). Wales Summit declaration [Press Release]. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_112964.htm

Newcomb, A. (2014, November 28). How Syrian Electronic Army pulled off Thanksgiving day hacks. *ABC News*. Retrieved from http://abcnews.go.com

Obama, B. (2015, January). State of the Union Address. Presented at U.S. Congress, Washington, D.C.

Office of the Secretary of Defense, Operational Test & Evaluation. (2015). *FY 2014 annual report*. Retrieved from http://www.dote.osd.mil/pub /reports/FY2014/pdf/other/2014DOTEAnnualReport.pdf

Ollman, G. (2009, August). Want to rent an 80–120k DDoS Botnet? [Blog Post]. Retrieved from https://blog.damballa.com/archives/330

Patrikakis, C., Masikos, M., Zouraraki, O. (2004). Distributed denial of service attacks. *The Internet Protocol Journal*. 7(4), 13–35.

Postel, J. (1981). *RFC 791: Internet protocol*. Internet Engineering Task Force, Fremont, CA.

Réseaux IP Européens Network Coordination Centre. (2008). *YouTube Hijacking: A RIPE NCC RIS case study*. Retrieved from http://www.ripe.net/Internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.

Rogers, M. (2015, February). Secretary of the Navy Guest Lecture. Presented at Naval Postgraduate School, Monterey, CA.

Rowe, N. C. (2010, January). The ethics of cyberweapons in warfare. *International Journal of Technoethics*, 1(1), 21–30.

Rowe, N. C. (2010, January). Towards reversible cyberattacks. In *Proceedings of the 9th European Conference on Information Warfare and Security* (pp. 261–267). Academic Conferences Limited.

Sale, R. (2012, October 19). Saudi insider likely key to Aramco cyber-attack. *Inter Press Service New Agency*. Retrieved from http://www.ipsnews.net

SCADA history. (2012, April 24). Retrieved from http://energy.sandia.gov/infrastructure-security/cyber/scada-systems/program-overview/scada-history/

Schelling, T.C. (2008). *Arms and influence*. New Haven, CT: Yale University Press.

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare.* Cambridge University Press.

Senie, D. (1999). *RFC 2644: Changing the default for directed broadcasts in routers*. Internet Engineering Task Force, Fremont, CA.

Songini, M. L. (2004, June 26). Supply chain system failures hampered Army units in Iraq. Computer World. Retrieved from http://www.computerworld.com/article/2566843/enterprise-resource-planning/supply-chain-system-failures-hampered-army-units-in-iraq.html.

Symantec. (2014). *Internet threat security report 2014* (19). Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

TCP SYN flooding and IP spoofing attacks. (2000). Retrieved from http://www.cert.org/historical/advisories/ca-1996-21.cfm

Team Cymru's Threat Intelligence Group. (2013). *Soho Pharming*. Retrieved from https://www.team-cymru.com/ReadingRoom/Whitepapers/2013/TeamCymruSOHOPharming.pdf

Thompson, N. (2013, May 8). Why did Syria shut down the Internet? *The New Yorker*. Retrieved from http://www.newyorker.com

TippingPoint Zero Day Initiative. (n.d.). Retrieved from http://www.zerodayinitiative.com

Tomahawk Cruise Missile fact sheet. (2014, August 14). Retrieved from http://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=1300&ct=2

Tzu, S. (1963). *The art of war*. Translated by Samuel B. Griffith. New York: Oxford University.

unixfreaxjp. (2014, January 3). Threat intelligence - New locker: prison locker (aka: Power locker ..or whatever those bad actor call it) [Blog Post]. Retrieved from http://blog.malwaremustdie.org/2014/01/threat-intelligence-new-locker-prison.html

Warren, M., & Hutchinson, W. (2000). Cyber attacks against supply chain management systems: a short note. *International Journal of Physical Distribution & Logistics Management*, 30(7/8), 710–716.

Weiss, T. G. (1999). Sanctions as a foreign policy tool: Weighing humanitarian impulses. *Journal of Peace Research*. 36(5), 499–509.

Wilson, Tim. (2010, August 3). Building botnets for fun and profit. *Dark Reading*. Retrieved from http://www.darkreading.com

Zetter, K. (2013, March 21). Logic bomb set off South Korea cyberattack. Wired. Retrieved from http://www.wired.com

Zhu, B., Joseph, A., & Sastry, S. (2011, October). A taxonomy of cyber attacks on SCADA systems. In *Internet of Things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing* (pp. 380–388). IEEE.

Zhu, Z., Lu, G., Chen, Y., Fu, Z., Roberts, P., & Han, K. (2008, July). Botnet research survey. In *Computer Software and Applications, 2008. COMPSAC'08. 32nd Annual IEEE International* (pp. 967–972). doi: 10.1109/COMPSAC.2008.205

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California